ServerIron ADX

Firewall Load Balancing Guide

Supporting Brocade ServerIron ADX version 12.4.00

BROCADE

Brocade Communications Systems, Incorporated

Document History

Title	Publication number	Summary of changes	Date
ServerIron ADX Firewall Load Balancing Guide	*53-1002380-01*	New document	July 2011
ServerIron ADX Firewall Load Balancing Guide	*53-1002436-01*	Updated to support FWLB for IPv6.	January 2012

Contents

Chapter 6   **Configuring FWLB and SLB**

Chapter 7   **Viewing FWLB Configuration Details and Statistics**

About This Document

In this chapter

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 switch, you should be familiar with the following protocols if applicable to your network: IP, RIP, OSPF, BGP, IS-IS, IGMP, PIM, DVMRP, and VRRP.

Supported hardware and software

The following hardware platforms are supported by this release of this guide:

- ServerIron ADX 1000
- ServerIron ADX 4000
- ServerIron ADX 8000
- ServerIron ADX 10000

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for 12.4 documenting all possible configurations and scenarios is beyond the scope of this document.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold; for example, **show version**.

Command syntax conventions

Command syntax in this manual follows these conventions:

command and **parameters**	Commands and parameters are printed in bold.
[ ]	Optional parameter.
<variable>	Variables are printed in italics enclosed in angled brackets < >.
...	Repeat the previous element, for example "member[;member...]"
|	Choose from one of the parameters.

Notes, cautions, and danger notices

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Sun Microsystems	Solaris
Microsoft Corporation	Windows NT, Windows 2000
The Open Group	Linux

Related publications

The following Brocade documents supplement the information in this guide:

- *Release Notes for ServerIron Switch and Router Software TrafficWorks 12.2.1*
- *ServerIron ADX Graphical User Interface Guide*
- *ServerIron ADX Server Load Balancing Guide*
- *ServerIron ADX Advanced Server Load Balancing Guide*
- *ServerIron ADX Global Server Load Balancing Guide*
- *ServerIron ADX Security Guide*
- *ServerIron ADX Administration Guide*
- *ServerIron ADX Switch and Router Guide*
- *ServerIron Chassis Hardware Installation Guide*
- *IronWare MIB Reference*

Getting technical help or reporting errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance, or find errors in the manuals, contact Brocade using one of the following options.

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the **Product Documentation** tab, and then click the link to the Knowledge Portal (KP). Then click **Cases** > **Create a New Ticket** to report an error. Make sure you specify the document title in the ticket description.

E-mail and telephone access

Go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

ServerIron FWLB Overview

In this chapter

Understanding ServerIron FWLB

Firewall Load Balancing (FWLB) allows the ServerIron ADX to balance traffic on multiple firewalls. The ServerIron ADX supports the following IPv4 FWLB topologies: Basic FWLB, High Availability (HA) FWLB, and Multizone FWLB.

NOTE
The ServerIron ADX supports the following IPv4 topologies: FWLB + NAT, FWLB + SYN Proxy, FWLB + L4 SLB.

NOTE
The ServerIron ADX supports the following IPv6 FWLB topologies: Basic FWLB and High Availability (HA) FWLB.

NOTE
IPv6 FWLB is only available on the Router Image.

You can configure FWLB for IPv6 topologies; however, the command line interface (CLI) does not accept IPv6 addresses for all commands. Table 1 provides a list of affected commands that enable you to configure IPv6 FWLB as well as the show commands.

TABLE 1 Commands affected by IPv6

Command	Definition/Example
`[no] server fw-name <name> <ipv6-addr>`	Use this command to configure an IPv6 firewall. ServerIronADX(config)# server fw-name ip6fw1 1113::2 ServerIronADX(config-rs-ip6fw1)# end ServerIronADX(config)# server fw-name ip6fw2 1113::3 ServerIronADX(config-rs-ip6fw2)# end For more information, refer to "Defining the firewalls and adding them to the firewall group" on page 18.
`[no] server fw-group 4 ipv6`	Use this command to configure an IPv6 firewall group. ServerIronADX(config)# server fw-group 4 ipv6 ServerIronADX(config-fw-4)# fw-name ip6fw1 ServerIronADX(config-fw-4)# fw-name ip6fw2 For more information, refer to "Defining the firewalls and adding them to the firewall group" on page 18.
`[no] fwall-info <path-num> <portnum> <other-ipv6> <next-hop-ipv6>`	Use this command to configure IPv6 firewall paths. ServerIronADX(config-fw-4)# fwall-info 1 8 1113::2 1112::2 ServerIronADX(config-fw-4)# fwall-info 2 9 1113::3 1112::3 SI-External(config-fw-4)# fw-predictor per-service-least-conn SI-External(config-fw-4)# exit For more information, refer to "Configuring the paths and adding static MAC entries" on page 20.
`[no] hash-mask <src-ipv6-mask> <dest-ipv6-mask>`	Use this command to configure the destination mask and source mask. ServerIronADX(config)# server fw-group 4 ServerIronADX(config-fw-4)# hash-mask FFFF:FFFF:FFFF::0 FFFF:FFFF:FFFF::0 ServerIronADX(config-fw-4)# end For more information, refer to "Overriding the global hash values" on page 172.
`[no] show fw hash <src-ipv6-mask> <dest-ipv6-mask> <firewall group>`	Use this command to show the destination mask or source mask. show fw hash FFFF:FFFF:FFFF::0 FFFF:FFFF:FFFF::0 4 For more information, refer to "Displaying the firewall selected by the hashing process for load balancing" on page 162.
`[no] other-ip <ipv6-addr>`	Use this command to identify the partner ServerIron ADX's firewall address. ServerIronADX(config)# server fw-name ip6fw1 1111::2 ServerIronADX(config-rs-fw1)# other-ip 1112::2 ServerIronADX(config-rs-fw1)# end For more information, refer to "Configuring active-active HA FWLB" on page 56.
`[no] policy-hash-acl <acl-name> <dest-ipv6-mask> <src-ipv6-mask>`	Use this command to configure the destination and source hash mask. ServerIronADX(config)# server fw-group 4 ServerIronADX(config-fw-4)# policy-hash-acl Ac2 FFFF:FFFF:FFFF:FFFF::0 FFFF:FFFF:FFFF:FFFF::0 ServerIronADX(config-fw-4)# end For more information, refer to "Overriding the global hash values" on page 172.
`[no] show fw-group`	Use this command to display firewall group details. ServerIronADX(config)#show fw-group For more information, refer to "Overriding the global hash values" on page 172.

TABLE 1   Commands affected by IPv6

Command	Definition/Example
`[no] show fw-health-check-stats`	Use this command to display firewall group health check statistics. `ServerIronADX 3018# show fw-health-check-stats` For more information, refer to "Displaying firewall health check policy statistics" on page 9.

`[no] debug fwlb ipv6 health-check`	Use these commands to debug a firewall group health check.
	`ServerIronADX_3007#debug fwlb ipv6 health-check`
	`ServerIronADX_3007#show debug`
	For more information, refer to "Firewall health check debug" on page 10.

`[no] debug fwlb ipv6 health-check-error`	Use these commands to debug a firewall group health check errors.
	`ServerIronADX_3007#debug fwlb ipv6 health-check-error`
	`ServerIronADX_3007#show debug`
	For more information, refer to "Firewall health check debug" on page 10.

To see examples of IPv6 configurations, refer to the following:

- "IPv6 example for basic Layer 3 FWLB" on page 24
- "IPv6 example for FWLB with one sub-net and one virtual routing interface" on page 29
- "IPv6 example for FWLB with multiple sub-nets and virtual routing interfaces" on page 34

Firewall environments

ServerIron supports load balancing across the following firewall environments:

Synchronous firewall environments

In general, firewalls that are synchronized allow the in and out traffic of conversations to pass through multiple firewalls. The firewalls exchange information about the conversation so that the inbound or outbound traffic for the conversation does not need to be revalidated each time it tries to use a different firewall. Although the firewalls themselves are synchronized, you will still need to configure paths on the ServerIron ADXs.

Asynchronous firewall environments

Asynchronous firewalls do not exchange information about conversations. New traffic must be revalidated each time it arrives at a new firewall. The path information you configure on the ServerIron ADX ensures that the traffic for a flow is sent to the firewall associated with that flow, thus reducing the overhead caused by needless revalidations.

NAT firewall environments

Firewalls that perform NAT can translate private network addresses (for example, 10.0.0.1) on the private side of the firewall into Internet addresses (for example, 209.157.22.26) on the public side of the firewall.

Dynamic route environments

ServerIrons in IronClad (high-availability) configurations automatically block Layer 3 route traffic at the backup ServerIron to avoid loops, thus simplifying configuration in these environments. Refer to "Router paths" on page 13.

Static route environments

Firewalls in static route environments have static or default routes, as do the external (Internet) and internal routers.

Layer 2 firewall environments

Layer 2 firewalls do not route (as Layer 3 firewalls do), so the path configuration is slightly different from the path configuration for Layer 3 firewalls.

NOTE
Layer 2 firewalls are only supported for IPv4.

NOTE
In all types of FWLB configurations, the ServerIrons must be able to reach the firewalls at Layer 2. Thus, the firewalls must be directly attached to the ServerIrons or attached to them through Layer 2 devices.

Load balancing paths

To send traffic through firewalls, the ServerIron ADX uses paths. A path consists of the following information:

- Path ID – The path ID is a number that identifies the path. In a basic FWLB configuration, the paths go from one ServerIron ADX to the other through the firewalls. In IronClad FWLB, additional paths go to routers. On each ServerIron ADX, the path IDs must be contiguous (with no gaps), starting with path ID 1.

- ServerIron ADX port – The number of the port that connects the ServerIron ADX to the firewall. The port number specified can be either the physical port number connected to the firewall or a dynamic port number 65535 that allows for the ServerIron ADX to dynamically detect the port to which the firewall is connected.

- Destination IP address – The management address of the ServerIron or Layer 2 switch on the other side of the firewall. The ServerIron ADX on the private network side and the other ServerIron ADX or Layer 2 switch are the endpoints of the data path through the firewall. If the path goes to a router, this parameter is the IP address of the firewall's interface with the ServerIron ADX.

- Next-hop IP address – The IP address of the firewall interface connected to this ServerIron ADX.

Figure 1 shows an example of FWLB paths.

FIGURE 1   Example of FWLB paths
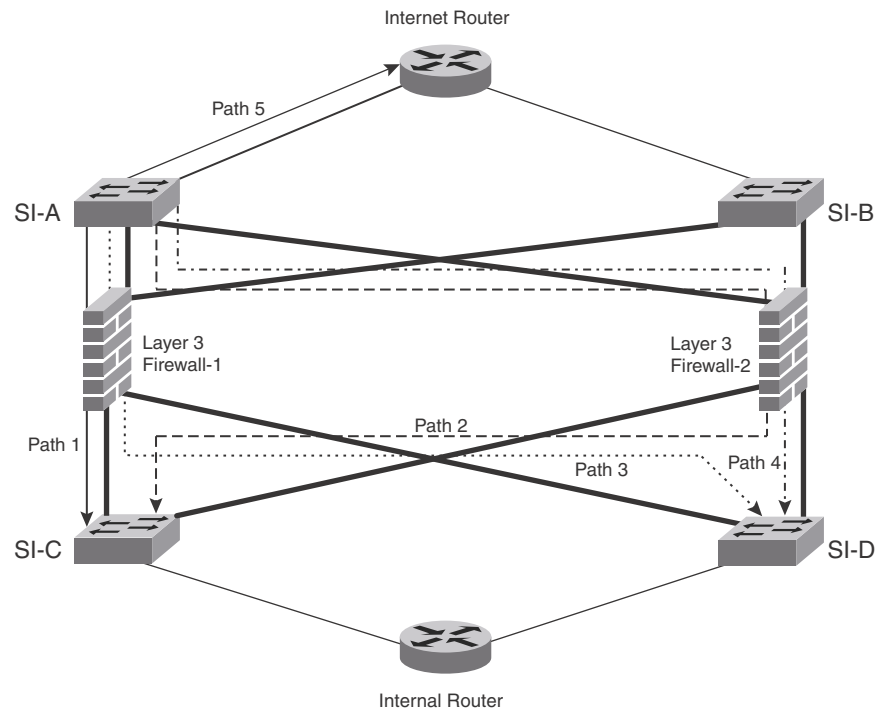
This example shows the following paths:

- Path 1—ServerIron ADX A through Firewall 1 to ServerIron C
- Path 2—ServerIron ADX A through Firewall 2 to ServerIron C
- Path 3—ServerIron ADX A through Firewall 1 to ServerIron D
- Path 4—ServerIron ADX A through Firewall 2 to ServerIron D
- Path 5—ServerIron ADX A to Internet router

To ensure proper synchronization of traffic through the firewalls, the paths must be symmetrical. This means that on each ServerIron ADX, the order of next-hop addresses must match. Thus, if you are configuring IronClad FWLB for Layer 3 firewalls, you must configure the paths so that the firewall interfaces are listed in the same order. For example, if the configuration contains four firewalls and you number them 1 through 4 from left to right, the paths on each ServerIron ADX must be configured so that the firewalls' next-hop addresses match (the interface for firewall 1 is in the first path, the interface for firewall 2 is in the second path, and so on).

Firewall selection

Once a ServerIron ADX has selected a firewall for a given traffic flow (source-destination pair of IP addresses), the ServerIron ADX uses the same firewall for subsequent traffic in the same flow.

For example (using IPv4 addresses), if the ServerIron ADX selects firewall FW1 for the first packet the ServerIron ADX receives with source address 1.1.1.1 and destination address 2.2.2.2, the ServerIron ADX uses FW1 for all packets of flows from 1.1.1.1 to 2.2.2.2.

For example (using IPv6 addresses), if the ServerIron ADX selects firewall FW2 for the first packet the ServerIron ADX receives with source address 1000::1 and destination address 2000::2, the ServerIron ADX uses FW2 for all packets of flows from 1000::1 to 2000::2.

The ServerIron ADX uses one of the following methods to select a firewall for the first packet:

- Select the firewall based on a hash calculation – Used for stateless FWLB
- Select the firewall with the fewest open connections – Used for stateful FWLB
- Select the firewall with the fewest open connections per service – Used for stateful FWLB

Hashing mechanism

The ServerIron ADXs use the path information along with the hash mask value for each source-destination pair of IP addresses in the user traffic to consistently send the same source-destination pairs through the same paths. For FWLB, the hash mask must be set to all ones (255.255.255.255 255.255.255.255 for IPv4 and FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF for IPv6) to ensure that a given source-destination pair always goes down the same path.

The ServerIron ADX selects a firewall for forwarding a packet based on the packet's hash value (the binary sum of the source and destination addresses). Once the ServerIron ADX assigns a hash value to a given source-destination pair, the ServerIron ADX associates that hash value with a path and always uses the same path for the source-destination pair that has the assigned hash value.

Hashing based on TCP or UDP port

You can configure the ServerIron ADX to hash based on destination TCP or UDP ports. When the ServerIron ADX uses the TCP or UDP port number in addition to the source and destination IP address, traffic with the same source and destination IP address can be load balanced across different paths, based on the destination TCP or UDP port number.

Stateful FWLB

A ServerIron ADX performs *stateful FWLB* by creating and using session entries for source and destination traffic flows and associating each flow with a specific firewall.

When a ServerIron ADX receives a packet that needs to go through a firewall, the ServerIron ADX checks to see whether it has an existing session entry for the packet:

- If the ServerIron ADX does not have a session entry with the packet's source and destination addresses, the ServerIron creates one. To create the session entry, the ServerIron ADX selects the firewall that has the fewest open sessions with the ServerIron ADX and associates the source and destination addresses of the packet with that firewall.

  The ServerIron ADX also sends the session information to the other ServerIron ADX in the high-availability pair, so that the other ServerIron ADX uses the associated path for the corresponding traffic and does not create a new session for the same traffic flow.

- If the ServerIron ADX already has a session entry for the packet, the ServerIron ADX forwards the traffic to the firewall in the session entry. All packets with the same source and destination addresses are forwarded to the same firewall. Because the ServerIron ADXs in a high-availability pair exchange session information, the same firewall is used regardless of which ServerIron ADX receives the traffic to be forwarded.

In addition to the firewall selection method based on fewest sessions described previously, a ServerIron ADX can also select a firewall that has the fewest open sessions for the requested service. For example, with "port http" defined for each firewall, HTTP requests will be load balanced to the firewall that has the least open HTTP connections.

Health checks

The ServerIron ADX regularly checks the health of the firewall paths and router paths, and of the applications on the firewalls, if you add applications to the firewall configurations.

ServerIron ADXs on each side of a firewall exchange health information for the links in each path by exchanging IP pings through the firewalls. When the ServerIron ADX on one side of a firewall receives a reply to a ping it sends to the other ServerIron ADX, on the other side of the firewall, the ServerIron ADX that sent the ping concludes that its partner on the other side of the firewall is operating normally.

The pings are required because a ServerIron ADX can use link-state information to detect when the local link (a link directly attached to a ServerIron ADX port) in a path goes down, but cannot detect when the remote link in the path goes down. If the other ServerIron ADX fails to respond to a ping on a specific port, the ServerIron ADX that sent the ping tries two more times, and then determines that the remote link in the path must be down.

NOTE

For Layer 3 health checks, the health-checking mechanism requires that the firewalls be configured to allow ICMP traffic between the two ServerIron ADXs and the ServerIron's gateway router. If the firewalls block the ICMP traffic between ServerIron ADXs, the health check will not work and, as a result, your IronClad configuration will not function properly.

Path health checks

One of the required FWLB parameters is a separate path from the ServerIron through each firewall to each of the ServerIrons on the other side of the firewall. A path to the ServerIron's gateway router also is required.

By default, the ServerIron ADX performs a Layer 3 health check of each firewall and router path by sending an ICMP ping packet on each path. Consider the following to determine the path:

- If the ServerIron ADX receives a reply within the allowed amount of time, the ServerIron ADX concludes that the path is good.

- If the ServerIron ADX does not receive a reply within the allowed amount of time, the ServerIron ADX concludes that the path is down.

By default, the ServerIron ADX waits 400 milliseconds for a reply to an ICMP health check packet. If the reply does not arrive, the ServerIron ADX makes two more attempts by default. Therefore, the total amount of time the ServerIron ADX waits for a response is 1.2 seconds by default.

You can increase the total amount of time the ServerIron will wait for a response by increasing the number of attempts. The default maximum number of health check attempts is 3. The valid number of attempts is a value from 3 through 31.

Optionally, you can configure the ServerIron ADXs in an FWLB configuration to use Layer 4 TCP or UDP health checks instead of Layer 3 health checks for firewall paths. When you configure a Layer 4 health check, the Layer 3 (ICMP) health check, which is used by default, is disabled. The Layer 4 health check applies only to firewall paths. The ServerIron ADX always uses a Layer 3 (ICMP) health check to test the path to the router.

NOTE
You must configure the same path health check parameters on all the ServerIron ADXs in the FWLB configuration. Otherwise, the paths will not pass the health checks.

Application health checks

When you add firewall configuration information to the ServerIron, you also can add information for individual application ports. Adding the application information is optional.

You can specify the following:

- The application's protocol (TCP or UDP) and port number
- The Layer 4 health check state (enabled or disabled) for the application

Adding an application port provides the following benefits:

- The ServerIron ADX includes the source and destination port numbers for the application when it creates a session entry. Thus, adding the application port provides more granular load balancing.
- The ServerIron ADX checks the health of the TCP or UDP service used by the application by sending a Layer 4 TCP or UDP health check to the firewall.

Layer 4 health checks are enabled by default. However, you can disable the Layer 4 health checks globally or on individual applications on individual firewalls.

The ServerIron performs the Layer 4 TCP and UDP health checks as follows:

- TCP health check – The ServerIron ADX checks the TCP port's health based on a TCP three-way handshake:
    - The ServerIron ADX sends a TCP SYN packet to the port on the firewall.
    - The ServerIron ADX expects the firewall to respond with a SYN ACK.
    - If the ServerIron ADX receives the SYN ACK, the ServerIron sends a TCP RESET, satisfied that the TCP port is alive.
- UDP health check – The ServerIron ADX sends a UDP packet with garbage (meaningless) data to the UDP port:
    - If the firewall responds with an ICMP "Port Unreachable" message, the ServerIron ADX concludes that the port is not alive.
    - If the server does not respond at all, the ServerIron ADX assumes that the port is alive and received the garbage data.

For more information about and configuration of health checks, refer to the *ServerIron ADX Server Load Balancing Guide*.

Firewall health check statistics

You can use the firewall health check statistics to analyze your firewall health checks.

Only statistics related to the firewall health check protocol (ICMP, TCP, and UDP) configured under a firewall group display. If the firewall group is disabled or unconfigured, the health check statistics related to that firewall group do not display.

Displaying firewall health check policy statistics

To display firewall health check policy statistics, enter the following command.

```
ServerIronADX 3018# show fw-health-check-stats

IPv4 Path Health Check Statistics:
==================================
ICMP : Requests Sent (10), Replies Received (10), Requests Received (10)
==================================
UDP Socket : Open Failed (0)
UDP Client : Requests Sent (16), Replies Received (16),  Replies Rx-Dropped (0)
UDP Server : Requests Received (16), Replies Sent (16), Requests Rx-Dropped (0)
==================================
TCP Socket : Client Connect Failed (0), Server Listen Failed (0)
TCP Client : Requests Sent (18), Replies Received (18), Replies Rx-Dropped (0)
TCP Server : Requests Received (18), Replies Sent (18), Requests Rx-Dropped (0)

IPv6 Path Health Check Statistics:
==================================
ICMP6 : Requests Sent (10), Replies Received (10), Requests Received (10)
==================================
UDP6 Socket : Open Failed (0)
UDP6 Client : Requests Sent (16), Replies Received (16),  Replies Rx-Dropped (0)
UDP6 Server : Requests Received (16), Replies Sent (16), Requests Rx-Dropped (0)
==================================
TCP6 Socket : Client Connect Failed (0), Server Listen Failed (0)
TCP6 Client : Requests Sent (18), Replies Received (18), Replies Rx-Dropped (0)
TCP6 Server : Requests Received (18), Replies Sent (18), Requests Rx-Dropped (0)
```

Syntax: show fw-health-check-stats

Table 2 displays the firewall health check statistics.

TABLE 2   Health-check policy statistics

Field	Description
Requests Sent	The number of health check packets sent.
Replies Received	The number of replies received.
Requests Received	The number of requests received.
Open Failed	The number of times the ServerIron ADX failed to open a connection.
Replies Rx-Dropped	The number of dropped replies received.
Client Connect Failed	The number of times the ServerIron ADX failed to connect to the client.
Server Listened Failed	The number of times the server listen failed.

Clearing health-check policy statistics

To clear firewall health check policy statistics, enter the following command.

```
ServerIronADX3018# clear fw-health-check-stats
```

Syntax: clear fw-health-check-stats

Firewall health check debug

To avoid cluttering the console with debug messages, health check debugs are automatically turned off after 30 seconds.

Use the following commands to debug your firewall health checks.

To debug an IPv4 firewall health check, enter the following command:

```
ServerIronADX_3007#debug fwlb ipv4 health-check
ServerIronADX_3007#show debug
```

To debug IPv4 firewall health check errors, enter the following command:

```
ServerIronADX_3007#debug fwlb ipv4 health-check-error
ServerIronADX_3007#show debug
```

To debug an IPv6 firewall health check, enter the following command:

```
ServerIronADX_3007#debug fwlb ipv6 health-check
ServerIronADX_3007#show debug
```

To debug IPv6 firewall health check errors, enter the following command:

```
ServerIronADX_3007#debug fwlb ipv6 health-check-error
ServerIronADX_3007#show debug
```

Syntax: debug fwlb ipv4 health-check | health-check-error

Syntax: debug fwlb ipv6 health-check | health-check-error

Basic FWLB topology

You can configure basic FWLB by deploying one ServerIron ADX on the enterprise side of the firewalls and another ServerIron ADX on the Internet side of the firewalls.

A basic FWLB topology uses two ServerIron ADXs to load balance traffic across Layer 3 firewalls. The firewalls can be synchronous or asynchronous.

In the basic configuration, one ServerIron ADX connects to all the firewalls on the private network side. The other ServerIron ADX connects to all the firewalls on the Internet side. The ServerIron ADXs balance firewall traffic flows across the firewalls.

Figure 2 shows an example of a basic FWLB topology.

FIGURE 2   **Basic FWLB topology**
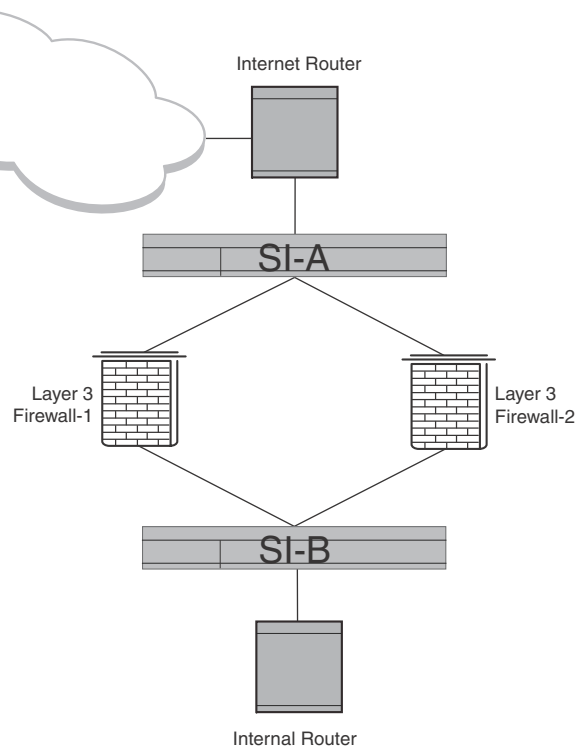
As shown in this example, each ServerIron ADX is configured with paths through the firewalls to the other ServerIron ADX. The ServerIron ADXs use these paths as part of the load balancing mechanism to ensure that traffic for a given IP source and IP destination always passes through the same firewall. All FWLB configurations require paths.

HA FWLB topology

For high availability (HA), you can deploy pairs of ServerIron ADXs in active-active configurations on each side of the firewalls. In an active-active configuration, both ServerIrons in a high-availability pair actively load balance FWLB traffic. Active-active operation provides redundancy in case a ServerIron ADX becomes unavailable, while enhancing performance by using both ServerIron ADXs to process and forward traffic.

HA FWLB on the ServerIron ADX must be in stateful. Each ServerIron ADX sends session information about its active traffic flows to the other ServerIron ADX. If a failover occurs, the ServerIron ADX that is still active can provide service for the other ServerIron traffic flows using the session information provided by the other ServerIron.

In an HA FWLB topology, both ServerIron ADXs actively load balance traffic to the firewalls. If one of the ServerIron ADXs becomes unavailable, the other ServerIron ADX automatically takes over load balancing for the sessions that were on the unavailable ServerIron ADX.

Figure 3 shows an example of HA FWLB topology.

FIGURE 3   HA FWLB topology
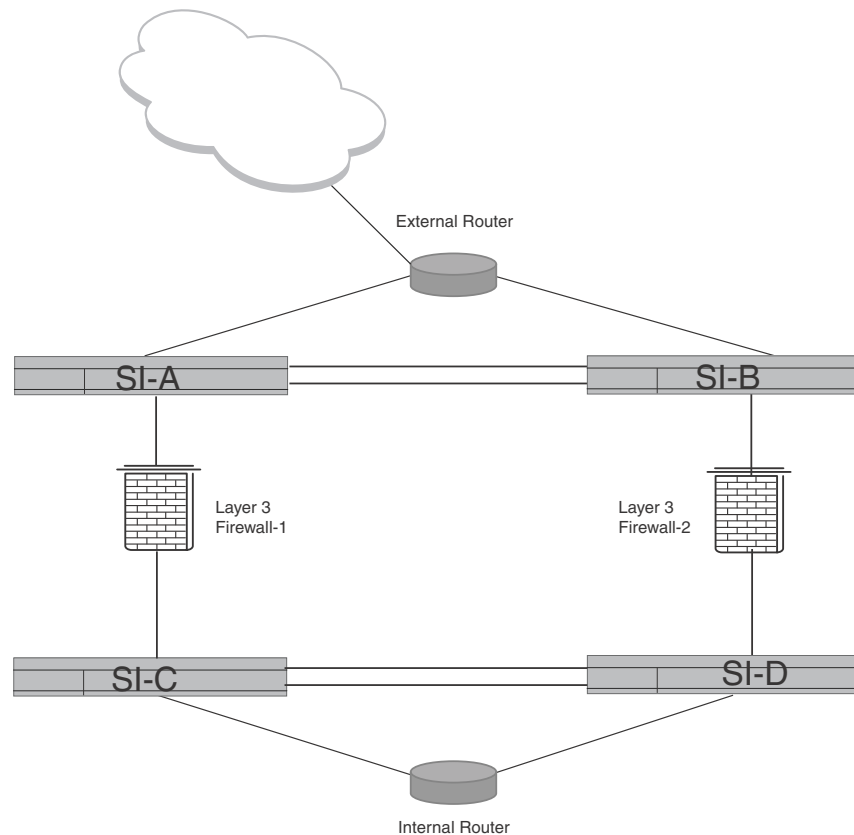
In this example, clients access the application servers on the private network through one of two routers, each of which is connected to a ServerIron ADX. The ServerIron ADXs create session entries for new traffic flows, including assignment of a firewall. The ServerIron ADXs then use the session entries to forward subsequent traffic in the flow to the same firewall.

Failover

In active-active FWLB, if one of the ServerIron ADXs becomes unavailable, the other ServerIron ADX takes over for the unavailable ServerIron ADX. The ServerIron ADXs uses the following parameter to manage failover:

ServerIron ADX priority – You can specify a priority from 0 through 255 on each ServerIron ADX. The ServerIron ADX with the higher priority is the default active ServerIron ADX. Specifying the priority is required.

NOTE
If you specify 0, the CLI removes the priority. When you save the configuration to the startup-config file, the **sym-priority** command is removed. Use this method to remove the priority. You cannot remove the priority using the **no sym-priority** command.

NOTE
The priority parameter does not apply to active-active configurations. However, you must configure the priority.

Router paths

IronClad FWLB configurations require paths to the routers in addition to paths to the firewalls. The router paths are required so the ServerIrons can ping the router links to assess their health.

In IronClad FWLB configurations, the standby ServerIron ADXs block Layer 3 OSPF, IGRP, and RIP traffic on the standby paths. This means that the ServerIrons block traffic between routers on different sides of the firewalls if the traffic uses the standby paths. After a failover to a standby ServerIron, the traffic pattern changes. The active ServerIron ADXs allow Layer 3 traffic between routers to pass through the firewalls on the active paths, while blocking the Layer 3 traffic on the standby paths.

NOTE
If you have configured a default route between the routers, the route will work only when the ServerIron through which the route passes is active. If the ServerIron is in standby mode, the route is blocked.

Multizone FWLB topology

> **NOTE**
> Multizone FWLB topology is only available for IPv4 address formats.

Figure 4 shows an example of Multizone basic FWLB.

FIGURE 4   Multizone basic FWLB
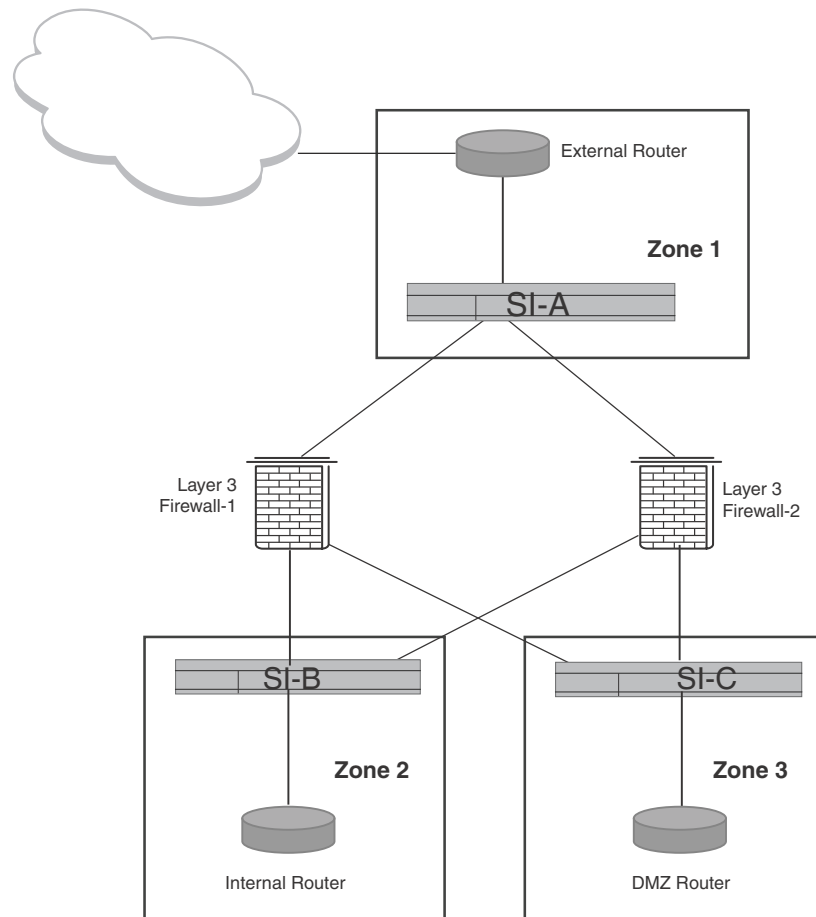
Figure 5 shows an example of Multizone HA FWLB.

FIGURE 5   Multizone HA FWLB
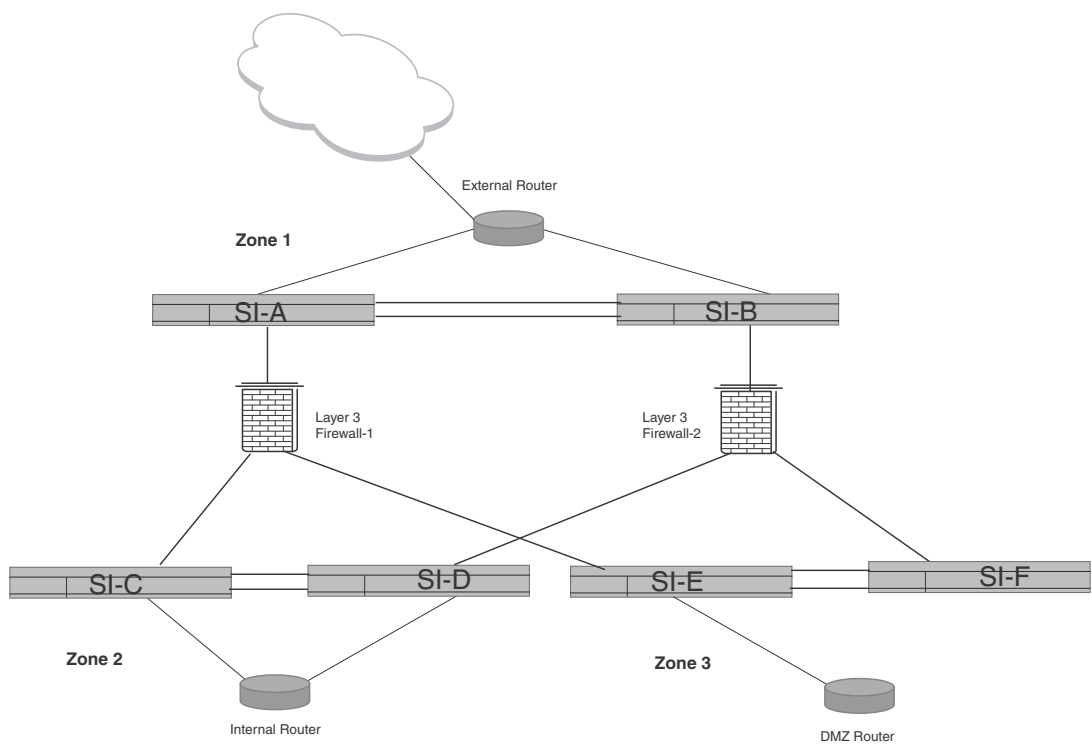
FWLB configuration limits

Table 3 contains the FWLB configuration limits supported by the ServerIron.

TABLE 3   FWLB configuration limits

Maximum firewall groups	Maximum firewalls	Maximum paths	Maximum zones	Maximum router paths
2 groups				
Group 2 - IPv4	16	64	8 (internal, external, dmz)	4
Group 4 - IPv6	16	64	1[a]	4

a.   Multizone for IPv6 is not supported.

Configuring Basic FWLB

In this chapter

Configuring basic Layer 3 FWLB

This chapter describes how to implement the following commonly used configurations:

- Basic FWLB (configuration without ServerIron ADX redundancy)
- IronClad (active-active configuration with ServerIron ADX redundancy)

Basic FWLB uses a single ServerIron ADX on the enterprise side of the load balanced firewalls and another ServerIron ADX on the Internet side. Figure 2 on page 11 shows an example of this type of configuration.

Configuration guidelines

Use the following guidelines when configuring a ServerIron ADX for FWLB:

- The ServerIron ADX supports two firewall groups, group 2 for IPv4 and group 4 for IPv6. All IPv4 ServerIron ADX ports must only belong to group 2 and all IPv6 ServerIron ADX ports must only belong to group 4.
- The ServerIron ADX must be able to reach the firewalls at Layer 2. Therefore, the firewalls must be either directly attached to the ServerIron ADX or connected through a Layer 2 switch.
- Static MAC entries for firewall interfaces are required. This is especially critical when the upstream Internet-side routers use the firewall interface as the next hop for reaching internal networks. These static entries are not necessary with ServerIron ADX router software and should not be used when a firewall path definition uses dynamic ports.
- Use "dynamic ports" with firewall path definitions when the firewall interface MAC address can be learned over different physical ports by the ServerIron ADX. Dynamic ports are only supported using IPv4 address formats.

- You must configure a separate path on each ServerIron ADX for each firewall. The paths ensure that firewall traffic with a given pair of source and destination IP addresses flows through the same firewall each time. Thus, the paths reduce firewall overhead by eliminating unnecessary revalidations.

NOTE
Path configuration is required for all load balancing configurations, whether the firewalls are synchronous or asynchronous.

Configuring basic Layer 3 FWLB

To configure basic Layer 3 FWLB, perform the tasks in Table 4.

TABLE 4   Basic Layer 3 configuration tasks

Task	Reference
Configure global parameters	
Configure firewall parameters	
Define the firewalls and add them to the firewall group	page 18
Configure firewall group parameters	
Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX	page 20

Defining the firewalls and adding them to the firewall group

When FWLB is enabled, all the IPv4 firewalls are in firewall group 2 and all the IPv6 firewalls are in firewall group 4. However, you need to add an entry for each firewall, and then add the firewalls to the appropriate firewall group. To add an entry for a firewall, specify the firewall name and the corresponding IPv4 or IPv6 address. You can specify a name up to 32 characters long.

To define the firewalls and add them to a firewall group, use the following methods:

- "IPv4 example for defining a firewall and adding them to a firewall group" on page 18
- "IPv6 example for defining a firewall and adding them to a firewall group" on page 19

IPv4 example for defining a firewall and adding them to a firewall group

To define the IPv4 firewalls, shown in Figure 2 on page 11, and add them to a firewall group, enter the following commands.

Commands for ServerIron ADX A (external)

```
ServerIron ADX(config)# server fw-name FW1-IPin 209.157.22.3
ServerIron ADX(config-rs-FW1-IPin)# exit
ServerIron ADX(config)# server fw-name FW2-IPin 209.157.22.4
ServerIron ADX(config-rs-FW2-IPin)# exit
ServerIron ADX(config)# server fw-group 2
ServerIron ADX(config-fw-2)# fw-name FW1-IPin
ServerIron ADX(config-fw-2)# fw-name FW2-IPin
```

Commands for ServerIron ADX B (internal)

```
ServerIron ADX(config)# server fw-name FW1-IPout 209.157.23.1
ServerIron ADX(config-rs-FW1-IPout)# exit
ServerIron ADX(config)# server fw-name FW2-IPout 209.157.23.2
ServerIron ADX(config-rs-FW2-IPout)# exit
ServerIron ADX(config)# server fw-group 2
ServerIron ADX(config-fw-2)# fw-name FW1-IPout
ServerIron ADX(config-fw-2)# fw-name FW2-IPout
```

Syntax: [no] server fw-name *<name>* *<ip-addr>*

NOTE
When you add a firewall name, the CLI level changes to the firewall level. This level is used when you configure stateful FWLB.

Syntax: (IPv4) **server fw-group 2**

These commands change the CLI to the firewall group configuration level. The IPv4 firewall group number is 2. Only one IPv4 firewall group is supported.

Syntax: [no] **fw-name** *<string>*

Adds a configured firewall to the firewall group.

IPv6 example for defining a firewall and adding them to a firewall group
To define the firewalls shown in Figure 2 on page 11 and add them to a firewall group, use the following method.

Commands for ServerIron ADX A (external)

```
ServerIron ADX(config)# server fw-name ip6fw1 1112::2
ServerIron ADX(config-rs-ip6fw1)# end
ServerIron ADX(config)# server fw-name ip6fw2 1112::3
ServerIron ADX(config-rs-ip6fw2)# end
ServerIron ADX(config)# server fw-group 4 ipv6
ServerIron ADX(config-fw-4)# fw-name ip6fw1
ServerIron ADX(config-fw-4)# fw-name ip6fw2
```

Commands for ServerIron ADX B (internal)

```
ServerIron ADX(config)# server fw-name ip6fw1 1113::2
ServerIron ADX(config-rs-ip6fw1)# end
ServerIron ADX(config)# server fw-name ip6fw2 1113::3
ServerIron ADX(config-rs-ip6fw2)# end
ServerIron ADX(config)# server fw-group 4 ipv6
ServerIron ADX(config-fw-4)# fw-name ip6fw1
ServerIron ADX(config-fw-4)# fw-name ip6fw2
```

Syntax: [no] **server fw-name** *<name>* *<ipv6-addr>*

NOTE
When you add a firewall name, the CLI level changes to the firewall level. This level is used when you configure stateful FWLB.

Syntax: (IPv6) [no] **server fw-group 4 ipv6**

These commands change the CLI to the firewall group configuration level. The IPv6 firewall group number is 4. Only one IPv6 firewall group is supported.

Syntax: [no] fw-name *<string>*

Adds a configured firewall to the firewall group.

Configuring the paths and adding static MAC entries

A path is configuration information the ServerIron ADX uses to ensure that a given source and destination IP pair is always authenticated by the same Layer 3 firewall.

Each path consists of the following parameters:

- The path ID – A number that identifies the path. The paths go from one ServerIron ADX to the other through the firewalls. On each ServerIron ADX, the sequence of path IDs must be contiguous (with no gaps), starting with path ID 1. For example, path sequence 1, 2, 3, 4, 5 is valid. Path sequence 1, 3, 5 or 5, 4, 3, 2, 1 is not valid.

- The ServerIron ADX port – The number of the port that connects the ServerIron ADX to the firewall. If your configuration does not require static MAC entries, you can specify a dynamic port (65535) instead of the physical port number for firewall paths. Specifying the dynamic port allows the ServerIron ADX to select the physical port for the path so you do not need to do so.

- The other ServerIron ADX's IP address – The IP address of the interface or the management address of the ServerIron ADX connected to this firewall. The ServerIron ADX on the private network side and the other ServerIron ADX are the endpoints of the data path through the firewall.

- The next-hop IP address – The IP address of the firewall interface connected to this ServerIron ADX.

> **NOTE**
> The other ServerIron's IP address and next-hop IP address parameters must be both IPv4 addresses or IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

> **NOTE**
> You must use IPv6 addresses for IPv6 firewalls and IPv4 addresses for IPv4 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

For each type of firewall (Layer 3 synchronous and asynchronous, with or without NAT), you must configure paths between the ServerIron ADXs through the firewalls.

In addition to configuring the paths, you must create a static MAC entry for each firewall interface attached to the ServerIron ADX.

> **NOTE**
> When defining a firewall router path on a port, make sure the port is a server router-port.

> **NOTE**
> FWLB paths must be fully meshed. When you configure a FWLB path on a ServerIron ADX, make sure you also configure a reciprocal path on the ServerIron ADX attached to the other end of the firewalls. For example, if you configure four paths to four separate firewalls, make sure you configure four paths on the other ServerIron ADX.

NOTE
For many configurations, static MAC entries are required. Where required, you must add a static MAC entry for each firewall interface with the ServerIron ADX. The FWLB configuration examples in this guide indicate whether static MAC entries are required.

To configure the paths and static MAC entries for the configuration shown in Figure 2 on page 11, enter the following commands. Note that the following example uses the IPv4 address format and firewall group 2. Enter the first group of commands on ServerIron ADX A. Enter the second group of commands on ServerIron ADX B.

Commands for ServerIron ADX A (external)
```
ServerIron ADX(config)# server fw-group 2
ServerIron ADX(config-fw-2)# fwall-info 1 3 209.157.23.3 209.157.22.3
ServerIron ADX(config-fw-2)# fwall-info 2 5 209.157.23.3 209.157.22.4
ServerIron ADX(config-fw-2)# exit
ServerIronADX(config)# vlan 1
ServerIron ADX(config-vlan-1)# static-mac-address abcd.4321.34e0 ethernet 3
priority 1 router-type
ServerIron ADX(config-vlan-1)# static-mac-address abcd.4321.34e1 ethernet 5
priority 1 router-type
ServerIron ADX(config)# write mem
```

Commands for ServerIron ADX B (internal)
```
ServerIron ADX(config)# server fw-group 2
ServerIron ADX(config-fw-2)# fwall-info 1 1 209.157.22.2 209.157.23.1
ServerIron ADX(config-fw-2)# fwall-info 2 2 209.157.22.2 209.157.23.2
ServerIron ADX(config-fw-2)# exit
ServerIronADX(config)# vlan 1
ServerIron ADX(config-vlan-1)# static-mac-address abcd.4321.34e2 ethernet 1
priority 1 router-type
ServerIron ADX(config-vlan-1)# static-mac-address abcd.4321.34e3 ethernet 2
priority 1 router-type
ServerIron ADX(config)# write mem
```

Syntax: (IPv4) server fw-group 2

Syntax: (IPv4) [no] fwall-info *<path-num> <portnum> <other-ip> <next-hop-ip>*

Syntax: (IPv6) server fw-group 4 ipv6

Syntax: (IPv6) [no] fwall-info *<path-num> <portnum> <other-ipv6> <next-hop-ipv6>*

NOTE
The other ServerIron ADX's IP address and next-hop IP address parameters must be both IPv4 addresses or both IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

NOTE
You must use IPv4 addresses for IPv4 firewalls and IPv6 addresses for IPv6 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

The *<path-num>* parameter specifies the path. The sequence of path IDs must be contiguous from start to finish.

The *<portnum>* parameter specifies the port that connects the ServerIron ADX to the firewall. If the port number is dynamic, use port number 65535.

The *<other-ip>* parameter specifies the IPv4 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ip>* parameter specifies the IPv4 address of the firewall connected to this ServerIron ADX.

The *<other-ipv6>* parameter specifies the IPv6 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ipv6>* parameter specifies the IPv6 address of the firewall connected to this ServerIron ADX.

Syntax: [no] static-mac-address *<mac-addr>* ethernet *<portnum>* [priority *<0-7>*] [host-type | router-type]

The priority can be 0 through 7 (0 is lowest and 7 is highest). The default is **0**.

The entry type parameters include **host-type** and **router-type.**The default is **host-type**.

NOTE
The static MAC entries are required. You must add a static MAC entry for each firewall interface with the ServerIron ADX. In addition, you must use the **priority 1** and **router-type** parameters with the **static-mac-address** command. These parameters enable the ServerIron ADX to use the address for FWLB.

NOTE
If you enter the command at the global CONFIG level, the static MAC entry applies to the default port-based VLAN (VLAN 1). If you enter the command at the configuration level for a specific port-based VLAN, the entry applies to that VLAN and not to the default VLAN.

Configuration example for basic Layer 3 FWLB

The following sections show all the ServerIron ADX commands you would enter on each ServerIron ADX to implement the configuration shown in

IPv4 example for basic Layer 3 FWLB

The following example uses the IPv4 address format and firewall group 2.

Commands on ServerIron ADX A (external)

Enter the following commands to configure FWLB on ServerIron ADX A.

The following commands add two firewalls, FW1-IPin and FW2-IPin.

```
ServerIron ADXA(config)# server fw-name FW1-IPin 209.157.22.3
ServerIron ADXA(config-rs-FW1-IPin)# exit
ServerIron ADXA(config)# server fw-name FW2-IPin 209.157.22.4
ServerIron ADXA(config-rs-FW2-IPin)# exit
```

The following commands configure parameters for firewall group (group 2 for IPv4 addresses). The **fwall-info** commands configure the paths for the firewall traffic. Each path consists of a path ID, the ServerIron ADX port attached to the firewall, the IP address of the ServerIron ADX at the other end of the path, and the next-hop IP address (usually the firewall interface connected to this ServerIron ADX). Make sure you configure reciprocal paths on the other ServerIron ADX, as shown in the section containing the CLI commands for ServerIron ADX B.

NOTE
Path information is required even if the firewalls are synchronized.

The **fw-name** *<firewall-name>* command adds the firewalls to the firewall group.

```
ServerIron ADXA(config)# server fw-group 2
ServerIron ADXA(config-fw-2)# fw-name FW1-IPin
ServerIron ADXA(config-fw-2)# fw-name FW2-IPin
ServerIron ADXA(config-fw-2)# fwall-info 1 3 209.157.23.3 209.157.22.3
ServerIron ADXA(config-fw-2)# fwall-info 2 5 209.157.23.3 209.157.22.4
ServerIron ADXA(config-fw-2)# exit
```

The following commands add static MAC entries for the MAC addresses of the firewall interfaces connected to the ServerIron ADX. Notice that the QoS priority is configured as **priority 1** and the **router-type** parameter is specified. These parameters are required.

NOTE
To ensure proper operation, always configure the path IDs so that the IDs consistently range from the lowest path ID to the highest path ID for the firewalls. For example, in Figure 2 on page 11, the path IDs should range from lowest to highest beginning with the firewall interface at the upper left of the figure.

To ensure smooth operation, you might want to depict your firewalls in a vertical hierarchy as in Figure 2 on page 11, label the interfaces with their IP addresses, and then configure the paths so that the path IDs to the interfaces range from lowest to highest path ID starting from the uppermost firewall interface.

```
ServerIron ADXA(config-vlan-1)# static-mac-address abcd.4321.34e0 ethernet 3
priority 1 router-type
ServerIron ADXA(config-vlan-1)# static-mac-address abcd.4321.34e1 ethernet 5
priority 1 router-type
ServerIron ADXA(config)# write memory
```

Commands on ServerIron ADX B (internal)

Enter the following commands to configure FWLB on ServerIron ADX B. Notice that the **fwall-info** commands configure paths that are reciprocal to the paths configured on ServerIron ADX A. Path 1 on each ServerIron ADX goes through one of the firewalls, while path 2 goes through the other firewall.

```
ServerIron ADXB(config)# server fw-name FW1-IPout 209.157.23.1
ServerIron ADXB(config-rs-FW1-IPout)# exit
ServerIron ADXB(config)# server fw-name FW2-IPout 209.157.23.2
ServerIron ADXB(config-rs-FW2-IPout)# exit
ServerIron ADXB(config)# server fw-group 2
ServerIron ADXB(config-fw-2)# fw-name FW1-IPout
ServerIron ADXB(config-fw-2)# fw-name FW2-IPout
```

```
ServerIron ADXB(config-fw-2)# fwall-info 1 1 209.157.22.2 209.157.23.1
ServerIron ADXB(config-fw-2)# fwall-info 2 2 209.157.22.2 209.157.23.2
ServerIron ADXB(config-fw-2)# exit
ServerIronADXB(config)# vlan 1
ServerIron ADXB(config-vlan-1)# static-mac-address abcd.4321.34e2 ethernet 1
priority 1 router-type
ServerIron ADXB(config-vlan-1)# static-mac-address abcd.4321.34e3 ethernet 2
priority 1 router-type
ServerIron ADXB(config)# write memory
```

IPv6 example for basic Layer 3 FWLB

The following example uses the IPv6 address format and firewall group 4.

Commands for ServerIron ADX A (external)

Enter the following commands to configure FWLB on ServerIron ADX A.

```
ServerIron ADX(config)# server fw-name ip6fw1 1111::2
ServerIron ADX(config-rs-ip6fw1)# end
ServerIron ADX(config)# server fw-name ip6fw2 1111::3
ServerIron ADX(config-rs-ip6fw2)# end
ServerIron ADX(config)# server fw-group 4 ipv6
ServerIron ADX(config-fw-4)# fw-name ip6fw1
ServerIron ADX(config-fw-4)# fw-name ip6fw2
ServerIron ADX(config-fw-4)# fwall-info 1 8 1113::1 1112::2
ServerIron ADX(config-fw-4)# fwall-info 2 9 1113::1 1112::3
ServerIron ADX(config-fw-4)# fw-predictor total-least-conn
ServerIron ADX(config-rs-FW2)# end
```

Commands for ServerIron ADX B (internal)

Enter the following commands to configure FWLB on ServerIron ADX B.

```
ServerIron ADX(config)# server fw-name ip6fw1 1113::2
ServerIron ADX(config-rs-ip6fw1)# end
ServerIron ADX(config)# server fw-name ip6fw2 1113::3
ServerIron ADX(config-rs-ip6fw2)# end
ServerIron ADX(config)# server fw-group 4 ipv6
ServerIron ADX(config-fw-4)# fw-name ip6fw1
ServerIron ADX(config-fw-4)# fw-name ip6fw2
ServerIron ADX(config-fw-4)# fwall-info 1 8 1113::2 1112::2
ServerIron ADX(config-fw-4)# fwall-info 2 9 1113::3 1112::3
ServerIron ADX(config-fw-4)# fw-predictor total-least-conn
ServerIron ADX(config-rs-FW2)# end
```

Configuration examples with Layer 3 routing support

This section shows examples of commonly used ServerIron ADX basic FWLB deployments with Layer 3 configurations. The ServerIron ADXs in these examples perform Layer 3 routing in addition to Layer 2 and Layer 4–7 switching.

Generally, the steps for configuring Layer 4–7 features on a ServerIron ADX running Layer 3 are similar to the steps on a ServerIron ADX that is not running Layer 3. The examples focus on the Layer 3 aspects of the configurations.

This section contains the following configuration examples:

- "Basic FWLB with one sub-net and one virtual routing interface" on page 25
- "Basic FWLB with multiple sub-nets and multiple virtual routing interfaces" on page 31

Basic FWLB with one sub-net and one virtual routing interface

Figure 6 (IPv4) and Figure 7 (IPv6) show an example of a basic FWLB configuration in which each ServerIron ADX is in only one sub-net. On each ServerIron ADX, a virtual routing interface is configured on all the ports in VLAN 1 (the default VLAN), and an IP sub-net address is configured on the virtual routing interface.

The ServerIron ADX supports dynamic routing protocols, including RIP and OSPF. However, some firewalls do not support dynamic routing and instead require static routes. The network in this example assumes that the firewalls do not support dynamic routing. Because the network uses static routes, each ServerIron ADX is configured with an IP default route that uses one of the firewall interfaces as the next hop for the route.

In addition, the client and server in this network each use a firewall interface as the default gateway. When this is the case, you need to do one of the following:

- Configure each ServerIron ADX with static MAC entries for the firewall interfaces. This example uses the static entries.
- Configure the clients and servers to use the ServerIron ADX itself as the default gateway.

IPv4 example for FWLB with one sub-net and one virtual routing interface

The following sections show the CLI commands for configuring the basic FWLB implementation in .

FIGURE 6   Basic IPv4 FWLB in one subnet
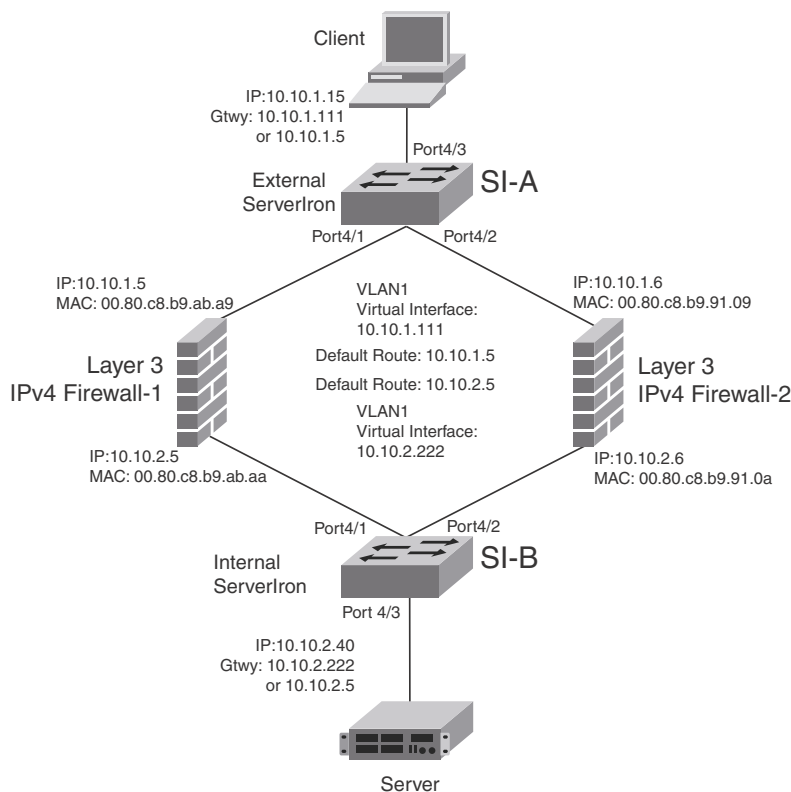
Commands on the external ServerIron ADX

The following commands change the CLI to the global CONFIG level, and then change the host name to "SI-External".

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-External
```

The following commands configure a virtual routing interface on VLAN 1 (the default VLAN), and then configure an IP address on the interface. The virtual routing interface is associated with all the ports in the VLAN. In this case, because all the ServerIron ADX ports are in the default VLAN, the virtual routing interface is associated with all the ports on the device.

```
SI-External(config)# vlan 1
SI-External(config-vlan-1)# router-interface ve 1
SI-External(config-vlan-1)# exit
SI-External(config)# interface ve 1
SI-External(config-ve-1)# ip address 10.10.1.111 255.255.255.0
SI-External(config-ve-1)# exit
```

The following command configures an IP default route. The first two "0.0.0.0" portions of the address are the IP address and network mask. Always specify zeroes when configuring an IP default route. The third value is the IP address of the next-hop gateway for the default route. In most cases, you can specify the IP address of one of the firewalls as the next hop. Specifying the default route is the Layer 3 equivalent of specifying the default gateway.

```
SI-External(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.5
```

The following commands add the firewall definitions. In this example, port HTTP is configured on each firewall. Specifying the application ports on the firewalls is optional. If you configure an application port on a firewall, load balancing is performed for the configured port. All traffic from a given client for ports that are not configured is sent to the same firewall.

```
SI-External(config)# server fw-name fw1 10.10.1.5
SI-External(config-rs-fw1)# port http
SI-External(config-rs-fw1)# exit
SI-External(config)# server fw-name fw2 10.10.1.6
SI-External(config-rs-fw2)# port http
SI-External(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group (group 2 for IPv4 addresses and group 4 for IPv6 addresses). The firewall group contains all the ports in VLAN 1 (the default VLAN).

```
SI-External(config)# server fw-group 2
SI-External(config-fw-2)# fw-name fw1
SI-External(config-fw-2)# fw-name fw2
```

The following commands add the paths through the firewalls to the other ServerIron ADX. Each path consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next-hop IP address. In this example, the topology does not contain routers other than the ServerIron ADXs. If your topology contains other routers, configure firewall paths for the routers too. For router paths, use the same IP address as the path destination and the next hop.

NOTE
The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
SI-External(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.5
SI-External(config-fw-2)# fwall-info 2 4/2 10.10.2.222 10.10.1.6
```

The following command sets the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. Because the previous firewall definitions specify the HTTP service, the ServerIron ADX will load balance requests based on the firewall that has fewer HTTP session entries in the ServerIron ADX session table.

```
SI-External(config-fw-2)# fw-predictor per-service-least-conn
SI-External(config)# exit
```

The following commands add static MAC entries for the firewall interfaces with the ServerIron ADX. The static MAC entries are required only if the configuration uses static routes and a single virtual routing interface, as in this example, and if the default gateway for the client or server is the firewall. If the configuration uses a dynamic routing protocol (for example, RIP or OSPF), the static entries are not required. Alternatively, the static entries are not required if you use the ServerIron ADX itself as the default gateway for the client or the server. For example, the static entries are not required if you configure the client to use 10.10.1.111 as its default gateway.

```
SI-External(config)# vlan 1
SI-External(config-vlan-1)# static-mac-address 0080.c8b9.aba9 ethernet 4/1
priority 1 router-type
SI-External(config-vlan-1)# static-mac-address 0080.c8b9.9109 ethernet 4/2
priority 1 router-type
SI-External(config-vlan-1)# exit
```

The following command saves the configuration changes to the startup-config file.

```
SI-External(config)# write memory
```

Commands on the internal ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-Internal
SI-Internal(config)# vlan 1
SI-Internal(config-vlan-1)# router-interface ve 1
SI-Internal(config-vlan-1)# exit
SI-Internal(config)# interface ve 1
SI-Internal(config-ve-1)# ip address 10.10.2.222 255.255.255.0
SI-Internal(config-ve-1)# exit
SI-Internal(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.5
SI-Internal(config)# server fw-name fw1 10.10.2.5
SI-Internal(config-rs-fw1)# port http
SI-Internal(config-rs-fw1)# exit
SI-Internal(config)# server fw-name fw2 10.10.2.6
SI-Internal(config-rs-fw2)# port http
SI-Internal(config-rs-fw2)# exit
SI-Internal(config)# server fw-group 2
SI-Internal(config-fw-2)# fw-name fw1
SI-Internal(config-fw-2)# fw-name fw2
SI-Internal(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.5
SI-Internal(config-fw-2)# fwall-info 2 4/2 10.10.1.111 10.10.2.6
SI-Internal(config-fw-2)# fw-predictor per-service-least-conn
SI-Internal(config)# exit
SI-Internal(config)# vlan 1
SI-Internal(config-vlan-1)# static-mac-address 0080.c8b9.abaa ethernet 4/1
priority 1 router-type
SI-Internal(config-vlan-1)# static-mac-address 0080.c8b9.910a ethernet 4/2
priority 1 router-type
SI-Internal(config-vlan-1)# exit
SI-Internal(config)# write memory
```

IPv6 example for FWLB with one sub-net and one virtual routing interface

The following sections show the CLI commands for configuring the basic IPv6 FWLB implementation in Figure 7.

FIGURE 7   Basic IPv6 FWLB in one subnet

Commands on the external ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-External
SI-External(config)# vlan 1
SI-External(config-vlan-1)# router-interface ve 1
SI-External(config-vlan-1)# exit
SI-External(config)# interface ve 1
SI-External(config-ve-1)# ip address 1112::1/64
SI-External(config-ve-1)# exit
SI-External(config)# ip route ::/0 ::/0 1113::3
SI-External(config)# server fw-name ip6fw1 1113::2
SI-External(config-rs-fw1)# port http
SI-External(config-rs-fw1)# exit
SI-External(config)# server fw-name ip6fw2 1113::3
SI-External(config-rs-fw2)# port http
SI-External(config-rs-fw2)# exit
SI-External(config)# server fw-group 4 ipv6
SI-External(config-fw-4)# fw-name ip6fw1
SI-External(config-fw-4)# fw-name ip6fw2
SI-External(config-fw-4)# fwall-info 1 8 1113::1 1112::2
SI-External(config-fw-4)# fwall-info 2 9 1113::1 1112::3
SI-External(config-fw-4)# fw-predictor per-service-least-conn
SI-External(config)# exit
```

```
SI-External(config)# vlan 1
SI-External(config-vlan-1)# static-mac-address 0080.c8b9.aba9 ethernet 4/1
priority 1 router-type
SI-External(config-vlan-1)# static-mac-address 0080.c8b9.9109 ethernet 4/2
priority 1 router-type
SI-External(config-vlan-1)# exit
SI-External(config)# write memory
SI-External(config)# end
```

Commands on the internal ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-Internal
SI-Internal(config)# vlan 1
SI-Internal(config-vlan-1)# router-interface ve 1
SI-Internal(config-vlan-1)# exit
SI-Internal(config)# interface ve 1
SI-Internal(config-ve-1)# ip address 1113::1/64
SI-Internal(config-ve-1)# exit
SI-Internal(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.5
SI-Internal(config)# server fw-name ip6fw1 1113::2
SI-Internal(config-rs-fw1)# port http
SI-Internal(config-rs-fw1)# exit
SI-Internal(config)# server fw-name ip6fw2 1113::3
SI-Internal(config-rs-fw2)# port http
SI-Internal(config-rs-fw2)# exit
SI-Internal(config)# server fw-group 4 ipv6
SI-Internal(config-fw-4)# fw-name ip6fw1
SI-Internal(config-fw-4)# fw-name ip6fw2
SI-Internal(config-fw-4)# fwall-info 1 8 1112::1 1113::2
SI-Internal(config-fw-4)# fwall-info 2 9 1112::1 1113::3
SI-Internal(config-fw-4)# fw-predictor per-service-least-conn
SI-Internal(config)# exit
SI-Internal(config)# vlan 1
SI-Internal(config-vlan-1)# static-mac-address 0080.c8b9.abaa ethernet 4/1
priority 1 router-type
SI-Internal(config-vlan-1)# static-mac-address 0080.c8b9.910a ethernet 4/2
priority 1 router-type
SI-Internal(config-vlan-1)# exit
SI-Internal(config)# write memory
SI-External(config)# end
```

Basic FWLB with multiple sub-nets and multiple virtual routing interfaces

Figure 8 (IPv4) and Figure 8 (IPv6) show an example of a basic FWLB configuration in which multiple IP sub-net interfaces are configured on each ServerIron ADX. On each ServerIron ADX, the client or server is in one sub-net and the firewalls are in another sub-net. The ports connected to the firewalls are configured in a separate port-based VLAN. The ServerIron ADX's IP interface to the firewalls is configured on a virtual routing interface associated with the ports in the VLAN.

The client and server in this example are each configured to use their locally attached ServerIron ADX as the default gateway, instead of using a firewall interface. Therefore, you do not need to configure static MAC entries for the firewalls on the ServerIron ADX.

IPv4 example for FWLB with multiple sub-nets and virtual routing interfaces

The following sections show the CLI commands for configuring the basic IPv4 FWLB implementation in Figure 8.

FIGURE 8   Basic IPv4 FWLB in multiple sub-nets using multiple routing interfaces
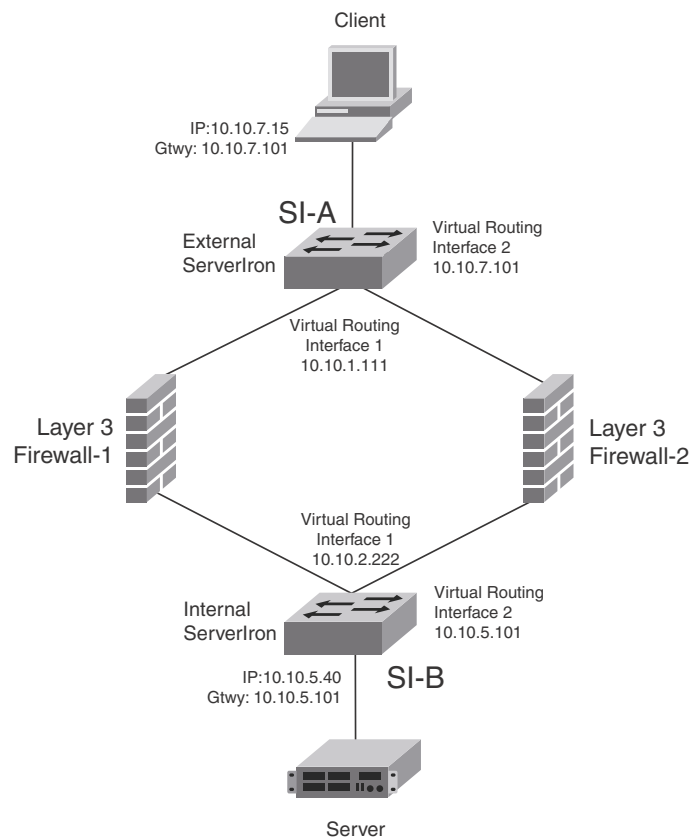
Commands on the external ServerIron ADX

The following commands change the CLI to the global CONFIG level, and then change the host name to "SI-External".

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-External
```

The following commands configure virtual routing interface 1, which is connected to the firewalls. Because both firewalls are in the same sub-net, you must configure the ServerIron ADX's IP interface with the firewalls on a virtual routing interface. Otherwise, you cannot configure the same address on more than one port.

The first three commands configure the VLAN. The last two commands configure an IP address on the interface. The IP address is assigned to all the ports in the VLAN associated with the virtual routing interface.

```
SI-External(config)# vlan 10
SI-External(config-vlan-10)# untagged ethernet 4/1 to 4/4
SI-External(config-vlan-10)# router-interface ve 1
SI-External(config-vlan-10)# exit
SI-External(config)# interface ve 1
SI-External(config-ve-1)# ip address 10.10.1.111 255.255.255.0
SI-External(config-ve-1)# exit
```

The following commands configure virtual routing interface 2, which is connected to the client.

```
SI-External(config)# vlan 20
SI-External(config-vlan-20)# untagged ethernet 4/5 to 4/24
SI-External(config-vlan-20)# router-interface ve 2
SI-External(config-vlan-20)# exit
SI-External(config)# interface ve 2
SI-External(config-ve-2)# ip address 10.10.7.101 255.255.255.0
SI-External(config-ve-2)# exit
```

Because Figure 8 on page 31 shows only one port connected to one client, you could configure the IP address on the physical port attached to the client instead of configuring the address on a separate VLAN. This example uses a virtual routing interface to demonstrate that you can use multiple virtual routing interfaces in your configuration.

The following command configures an IP default route. The first two "0.0.0.0" portions of the address are the IP address and network mask. Always specify zeroes when configuring an IP default route. The third value is the IP address of the next-hop gateway for the default route. In most cases, you can specify the IP address of one of the firewalls as the next hop. Specifying the default route is the Layer 3 equivalent of specifying the default gateway.

```
SI-External(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.5
```

The following commands add the firewall definitions.

```
SI-External(config)# server fw-name fw1 10.10.1.5
SI-External(config-rs-fw1)# port http
SI-External(config-rs-fw1)# exit
SI-External(config)# server fw-name fw2 10.10.1.6
SI-External(config-rs-fw2)# port http
SI-External(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group.

```
SI-External(config)# server fw-group 2
SI-External(config-fw-2)# fw-name fw1
SI-External(config-fw-2)# fw-name fw2
```

The following commands add the paths through the firewalls to the other ServerIron ADX. Each path consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next-hop IP address. In this example, the topology does not contain routers other than the ServerIron ADXs. If your topology contains other routers, configure firewall paths for the routers too. For router paths, use the same IP address as the path destination and the next hop.

NOTE
The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
SI-External(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.5
SI-External(config-fw-2)# fwall-info 2 4/2 10.10.2.222 10.10.1.6
```

The following command sets the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service.

```
SI-External(config-fw-2)# fw-predictor per-service-least-conn
SI-External(config-fw-2)# exit
```

The following command saves the configuration changes to the startup-config file.

```
SI-External(config)# write memory
```

Commands on the internal ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-Internal
SI-Internal(config)# vlan 10
SI-Internal(config-vlan-10)# untagged ethernet 4/1 to 4/4
SI-Internal(config-vlan-10)# router-interface ve 1
SI-Internal(config-vlan-10)# exit
SI-Internal(config)# interface ve 1
SI-Internal(config-ve-1)# ip address 10.10.2.222 255.255.255.0
SI-Internal(config-ve-1)# exit
SI-Internal(config)# vlan 20
SI-Internal(config-vlan-20)# untagged ethernet 4/5 to 4/24
SI-Internal(config-vlan-20)# router-interface ve 2
SI-Internal(config-vlan-20)# exit
SI-Internal(config)# interface ve 2
SI-Internal(config-ve-2)# ip address 10.10.5.101 255.255.255.0
SI-Internal(config-ve-2)# exit
SI-Internal(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.5
SI-Internal(config)# server fw-name fw1 10.10.2.5
SI-Internal(config-rs-fw1)# port http
SI-Internal(config-rs-fw1)# exit
SI-Internal(config)# server fw-name fw2 10.10.2.6
SI-Internal(config-rs-fw2)# port http
SI-Internal(config-rs-fw2)# exit
SI-Internal(config)# server fw-group 2
SI-Internal(config-fw-2)# fw-name fw1
SI-Internal(config-fw-2)# fw-name fw2
SI-Internal(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.5
SI-Internal(config-fw-2)# fwall-info 2 4/2 10.10.1.111 10.10.2.6
SI-Internal(config-fw-2)# fw-predictor per-service-least-conn
SI-Internal(config-fw-2)# exit
SI-Internal(config)# write memory
```

IPv6 example for FWLB with multiple sub-nets and virtual routing interfaces

The following sections show the CLI commands for configuring the basic IPv6 FWLB implementation in Figure 8.

FIGURE 9   Basic IPv6 FWLB in multiple sub-nets using multiple routing interfaces

Commands on the external ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-External
SI-External(config)# vlan 10
SI-External(config-vlan-10)# untagged ethernet 4/1 to 4/4
SI-External(config-vlan-10)# router-interface ve 1
SI-External(config-vlan-10)# exit
SI-External(config)# interface ve 1
SI-External(config-ve-1)# ip address 1112::1/64
SI-External(config-ve-1)# exit
SI-External(config)# vlan 20
SI-External(config-vlan-20)# untagged ethernet 4/5 to 4/24
SI-External(config-vlan-20)# router-interface ve 2
SI-External(config-vlan-20)# exit
SI-External(config)# interface ve 2
SI-External(config-ve-2)# ip address 1113::1/64
SI-External(config-ve-2)# exit
SI-External(config)# ip route ::/0 ::/0 1113::3
```

```
SI-External(config)# server fw-name ip6fw1 1113::2
SI-External(config-rs-fw1)# port http
SI-External(config-rs-fw1)# exit
SI-External(config)# server fw-name ip6fw2 1113::3
SI-External(config-rs-fw2)# port http
SI-External(config-rs-fw2)# exit
SI-External(config)# server fw-group 4 ipv6
SI-External(config-fw-4)# fw-name ip6fw1
SI-External(config-fw-4)# fw-name ip6fw2
SI-External(config-fw-4)# fwall-info 1 8 1113::1 1112::2
SI-External(config-fw-4)# fwall-info 2 9 1113::1 1112::3
SI-External(config-fw-4)# fw-predictor per-service-least-conn
SI-External(config-fw-4)# exit
SI-External(config)# write memory
```

Commands on the internal ServerIron ADX

```
ServerIron ADX> enable
ServerIron ADX# configure terminal
ServerIron ADX(config)# hostname SI-Internal
SI-Internal(config)# vlan 10
SI-Internal(config-vlan-10)# untagged ethernet 4/1 to 4/4
SI-Internal(config-vlan-10)# router-interface ve 1
SI-Internal(config-vlan-10)# exit
SI-Internal(config)# interface ve 1
SI-Internal(config-ve-1)# ip address 1113::1/64
SI-Internal(config-ve-1)# exit
SI-Internal(config)# vlan 20
SI-Internal(config-vlan-20)# untagged ethernet 4/5 to 4/24
SI-Internal(config-vlan-20)# router-interface ve 2
SI-Internal(config-vlan-20)# exit
SI-Internal(config)# interface ve 2
SI-Internal(config-ve-2)# ip address 1114::1/64
SI-Internal(config-ve-2)# exit
SI-Internal(config)# ip route 0::/0 ::/0 1113::2
SI-Internal(config)# server fw-name ip6fw1 1113::2
SI-Internal(config-rs-fw1)# port http
SI-Internal(config-rs-fw1)# exit
SI-Internal(config)# server fw-name ip6fw1 1113::3
SI-Internal(config-rs-fw2)# port http
SI-Internal(config-rs-fw2)# exit
SI-Internal(config)# server fw-group 4 ipv6
SI-Internal(config-fw-4)# fw-name ip6fw1
SI-Internal(config-fw-4)# fw-name ip6fw2
SI-Internal(config-fw-4)# fwall-info 1 8 1112::1 1113::2
SI-Internal(config-fw-4)# fwall-info 2 9 1112::1 1113::3
SI-Internal(config-fw-4)# fw-predictor per-service-least-conn
SI-Internal(config-fw-4)# exit
SI-Internal(config)# write memory
```

Configuring HA FWLB

In this chapter

Understanding ServerIron FWLB

High Availability (HA) FWLB allows the ServerIron ADX to actively load balance traffic and provide enhanced performance.

For basic information about FWLB, refer to the following sections:

• "Stateful FWLB" on page 7

• "Health checks" on page 7

Layer 3 or Layer 4 sessions

The source and destination addresses in a session entry are Layer 3 or Layer 4 session entries. Consider the following:

• A Layer 3 session entry contains source and destination IP addresses.

• A Layer 4 session entry contains source and destination TCP and UDP port numbers in addition to IP addresses.

The session entry type depends on whether you configure application ports (TCP or UDP ports) to the firewall configuration information on the ServerIron ADX:

• If you do not configure application ports on a firewall, the ServerIron ADX creates session entries using the source and destination IP addresses only. All packets for a given pair of source and destination IP addresses are always sent to the same firewall.

• If you configure an application port on a firewall, the ServerIron ADX includes the source and destination TCP or UDP port numbers in the session entries for the application. Packets for the same set of source and destination IP addresses can be sent to different firewalls, depending on the source and destination TCP or UDP port numbers in the packets. For example, if you configure TCP port 80 on the firewalls, the ServerIron ADX uses IP addresses and TCP port numbers in the session table entries for HTTP traffic.

Session limits

To avoid overloading a firewall, the ServerIron ADX does not forward a packet to a firewall if either of the following conditions exists:

- The firewall already has the maximum allowed number of open sessions with the ServerIron ADX. An open session is represented by a session entry. By default, a firewall can have up to two million session entries on the ServerIron ADX. In a high-availability pair, the firewall can have up to two million session entries combined on both ServerIron ADXs. You can change the maximum number of sessions on an individual firewall basis to a number from 1 through 2,000,000.

- The firewall has already received the maximum allowed number of new sessions within the previous one-second interval. By default, the ServerIron ADX will allow up to two million new sessions to the same firewall. The maximum includes TCP and UDP sessions combined. You can change the maximum number of sessions per-second separately for TCP and UDP, to a value from 1 through 2,000,000.

Session aging

The ServerIron ADX ages out inactive session entries. The aging mechanism differs depending on whether the session entry is a Layer 3 entry or a Layer 4 entry:

- Layer 3 session entries – The ServerIron ADX uses the sticky age timer to age out Layer 3 session entries. The default sticky age is 5 minutes. You can change the sticky age to a value from 2 through 60 minutes.

  - To change the timer, enter the **server sticky-age** *<num>* command at the global CONFIG level of the CLI.

- Layer 4 session entries – The ServerIron ADX clears a session entry that has TCP ports when the ServerIron ADX receives a TCP FIN or RESET to end the session. For a TCP session that ends abnormally, the ServerIron ADX uses the TCP age timer to age out the session. The ServerIron ADX uses the UDP age timer to age out all UDP sessions. The default TCP age timer is 30 minutes. The default UDP age timer is 5 minutes. You can configure either timer to a value from 2 through 60 minutes.

  - To change the TCP age timer, enter the **server tcp-age** *<num>* command at the global CONFIG level of the CLI.

  - To change the UDP age timer, enter the **server udp-age** *<num>* command at the global CONFIG level of the CLI.

NOTE
Server Load Balancing (SLB) uses the same values for the sticky age, TCP age, and UDP age timers. If you change a timer, the change applies to both SLB and FWLB.

Configuring HA active-active FWLB

This section contains the following sections:

Overview of active-active FWLB

Active-active operation provides redundancy in case a ServerIron ADX becomes unavailable, while enhancing performance by using both ServerIron ADXs to process and forward traffic.

NOTE
Active-active operation is not the same thing as the always-active feature. The always-active feature is used to simplify the topology of high-availability FWLB configurations, and can be used in an active-active configuration.

Figure 10 shows an example of ServerIron ADX chassis configured for high-availability FWLB.

FIGURE 10   HA FWLB for Layer 3 firewalls
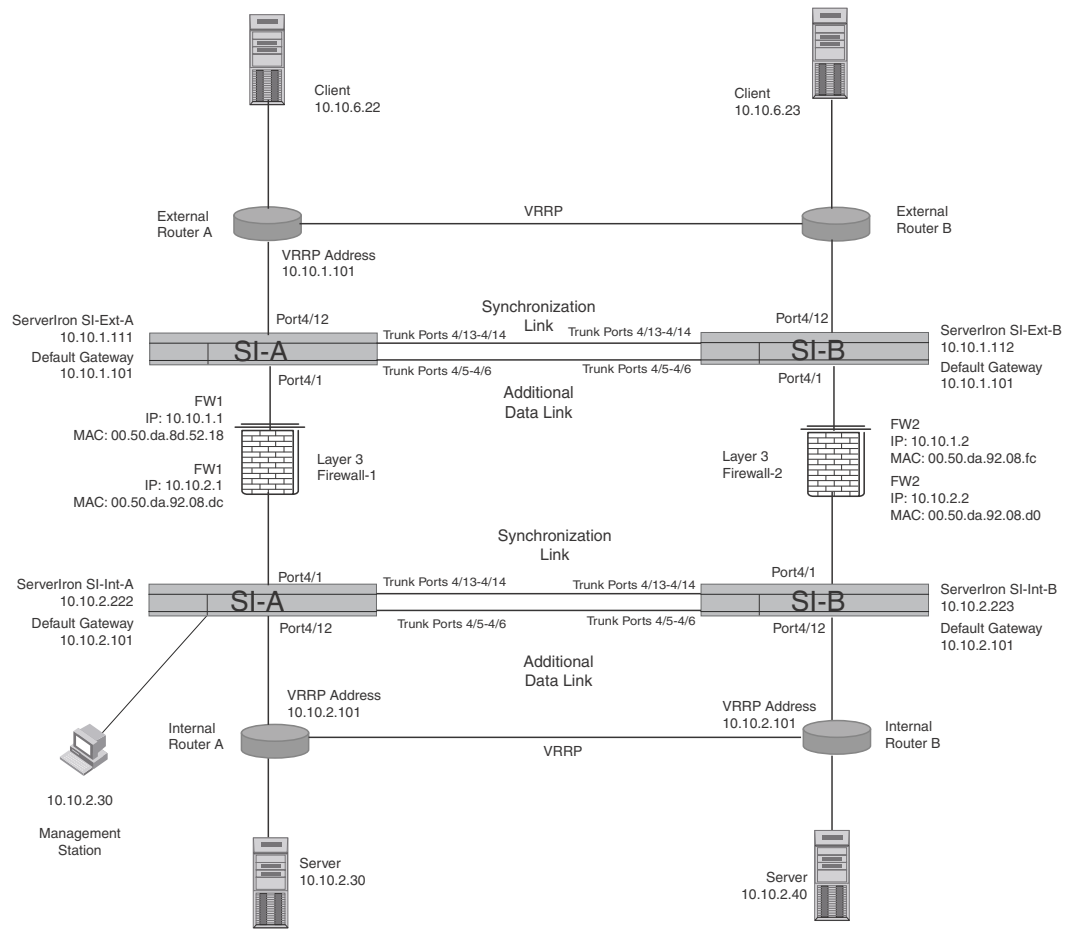
HA FWLB configuration guidelines

Use the following guidelines when configuring a ServerIron ADX for HA FWLB:

- The ServerIron ADX must be able to reach the firewalls at Layer 2. Therefore, the firewalls must be either directly attached to the ServerIron ADX or connected through a Layer 2 switch.

- The SYNC link between the two ServerIron ADX switches must always be in a separate VLAN. One must not tag this link to send data traffic over it.

- Firewall path definitions on each ServerIron ADX must be symmetrical. The order of next-hop addresses must match. For example, if the topology is comprised of outside and inside ServerIron ADX pairs and four firewalls, then on each ServerIron ADX, define the first path through firewall 1, the second path through firewall 2, and so on.

- Static MAC entries for firewall interfaces are required. This is especially critical when the upstream Internet side routers use the firewall interface as the next hop for reaching internal networks. These static entries are not necessary with ServerIron ADX router software and should not be used when a firewall path definition uses dynamic ports.

- Use "dynamic ports" with firewall path definitions when the firewall interface MAC address can be learned over different physical ports by the ServerIron ADX.

- You must use the **server partner-ports** command to identify the data path from a peer ServerIron ADX in HA.

- Do not combine FWLB with Layer 7 content switching features. The FWLB+TCS combination is also not supported.

In this example, clients access the application servers on the private network through one of two routers, each of which is connected to a ServerIron ADX. The ServerIron ADXs create session entries for new traffic flows, including assignment of a firewall. The ServerIron ADXs then use the session entries to forward subsequent traffic in the flow to the same firewall.

The ServerIron ADXs on the private side of the network are connected to the application servers through routers. These ServerIron ADXs also create session entries and use those entries for forwarding traffic to the servers, and the server replies back to the clients.

Each pair of ServerIron ADXs is connected by two trunk groups. One of the trunk groups is the synchronization link, and is used by the ServerIron ADX to exchange session information, so that each ServerIron ADX has a complete list of the sessions. If one of the ServerIron ADXs becomes unavailable, the other ServerIron ADX can continue FWLB service without interruption, even for existing sessions.

The other trunk group is an additional data link and allows for a simplified topology by eliminating the need for separate Layer 2 switches between the ServerIron ADXs and firewalls.

These links are not required to be trunk groups, but configuring them as trunk groups adds link-level redundancy to the overall redundant design.

The pairs of routers are configured with Virtual Router Redundancy Protocol (VRRP) to share the default gateway address used by the ServerIron ADXs attached to the routers.

A management station attached to one of the ServerIron ADXs on the private side of the firewalls provides Telnet management access to all four ServerIron ADXs.

To implement the active-active FWLB configuration shown in Figure 10, perform the tasks shown in Table 5 on each ServerIron ADX.

TABLE 5   Active-active FWLB configuration tasks

Task	Reference
Configure global parameters	
Configure the management IP address and default gateway	page 42
Configure the firewall port for the synchronization link	page 42
Configure the partner port for the data link	page 43
Configure the additional data link (the always-active link)	page 43
Configure the router port	page 44
Configure firewall parameters	
Define the firewalls and add them to the firewall group. When you define each firewall, optionally specify: - The TCP or UDP application ports on the firewall - The health check state (enabled by default) - The maximum total number of sessions - The maximum new session rate	page 44

TABLE 5   Active-active FWLB configuration tasks (Continued)

Task	Reference
Configure firewall group parameters	
Change the load balancing method from least connections to least connections per application (optional)	page 47
Enable the active-active mode	page 48
Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX	page 48
Configure the ServerIron ADX to drop traffic when the firewall has reached its maximum number of sessions or maximum new session rate (optional)	page 50
Configure the ServerIron ADX to forward a TCP data packet only if the ServerIron ADX has already received a TCP SYN for the packet's source and destination addresses (optional)	page 50

Configuring the management IP address and default gateway

You must add a management IP address to the ServerIron ADX and the IP address must be in the same sub-net as the ServerIron ADX's interfaces with the Layer 3 firewalls.

For the default gateway address, specify the IP address on the router's interface with the ServerIron ADX.

```
ServerIronADX(config)# ip address 10.10.1.111 255.255.255.0
ServerIronADX(config)# ip default-gateway 10.10.1.101
```

Syntax: ip address *<ip-addr> <ip-mask>*

or

Syntax: ip address *<ip-addr>***/***<mask-bits>*

Syntax: ip default-gateway *<ip-addr>*

Configuring the firewall port

When you configure the ServerIron ADX for IronClad FWLB, you must specify the port number of the dedicated synchronization link between the ServerIron ADX and its active-active partner. To specify the port, enter a command such as the following at the global CLI level.

```
ServerIronADX(config)# server fw-port 4/13
```

Syntax: [no] server fw-port *<portnum>*

If the link between the two ServerIron ADXs is a trunk group (recommended for added redundancy), specify the port number of the primary port. The primary port is the first port in the trunk group.

Configuring the partner port

Use the partner-ports command to configure the data link between the ServerIron and its active-active partner. You must use the server partner-ports command to specify all data links with the partner. To specify the partner port, enter the following command.

NOTE
Do not use the partner-ports command for the synchronization link.

```
SI-Ext-A(config)# server partner-ports ethernet 3/1
```

Syntax: [no] **server partner-ports** <*portnum*>

Configuring the additional data link (the always-active link)

The default port-based VLAN, VLAN 1, contains all the ServerIron ADX ports by default. In configurations such as the one shown in , the ports of the additional data link between the ServerIron ADXs in each pair also are in this VLAN. For this type of configuration, you must perform the following configuration steps for the default VLAN:

- Disable the Spanning Tree Protocol (STP)
- Enable the always-active option

To disable STP and enable the always-active feature, enter the following commands.

```
ServerIronADX(config)# vlan 1
ServerIronADX(config-vlan-1)# no spanning-tree
ServerIronADX(config-vlan-1)# always-active
ServerIronADX(config-vlan-1)# exit
```

Syntax: [no] **vlan** <*num*>

Syntax: [no] **spanning-tree**

Syntax: [no] **always-active**

NOTE
To use the always-active feature, you also must enable the L2-fwall feature at the firewall group configuration level.

Configuring the router port

> **NOTE**
> Do not configure the router-port in an active-active FWLB. Router-port configuration is a trigger (Router-cnt) that changes the FWLB status without the active-active HA configuration.

High-availability FWLB configurations require that you identify the ports on the ServerIron ADX that are attached to the routers. To identify the router port, enter the following command.

```
ServerIronADX(config)# server router-ports 4/12
```

Syntax: [no] **server router-ports** *<portnum>*

> **NOTE**
> To define multiple router ports on a switch, enter the port numbers separated by blanks. You can enter up to eight router ports in a single command line. To enter more than eight ports, enter the **server router-ports** command again with the additional ports.

If the link is a trunk group, specify the port number of the primary port. The primary port is the first port in the trunk group.

Configuring the firewalls

To configure a firewall, enter a name for the firewall and the IP address of its interface with the ServerIron ADX. Optionally, you also can enter the following information:

- The TCP or UDP application ports on the firewall
- The health check state (enabled by default)
- The maximum total number of sessions
- The maximum new session rate

Adding the firewalls

To configure the IPv4 firewalls on ServerIron ADX SI-Ext-A in Figure 10, enter the following commands.

```
ServerIronADX(config)# server fw-name FW1 10.10.10.1
ServerIronADX(config-rs-FW1)# port http
ServerIronADX(config-rs-FW1)# exit
ServerIronADX(config)# fw-name FW2 10.10.10.2
ServerIronADX(config-rs-FW2)# port http
ServerIronADX(config-rs-FW2)# exit
ServerIronADX(config)# server fw-group 2
ServerIronADX(config-fw-2)# fw-name FW1
ServerIronADX(config-fw-2)# fw-name FW2
```

Syntax: [no] **server fw-name** *<string>* *<ip-addr>*

This command adds a firewall.

Syntax: [no] **port** *<tcp/udp-port>* **[no-health-check]**

The *<tcp/udp-port>* parameter can be a number from 1 through 65535 or one of the following well-known port names:

- **dns** – port 53
- **ftp** – port 21 (Ports 20 and 21 are FTP ports but in the ServerIron ADX, the name "ftp" corresponds to port 21.)
- **http** – port 80
- **imap4** – port 143
- **ldap** – port 389
- **nntp** – port 119
- **ntp** – port 123
- **pop2** – port 109
- **pop3** – port 110
- **radius** – UDP port 1812
- **radius-old** – The ServerIron ADX name for UDP port 1645, which is used in some older RADIUS implementations instead of port 1812
- **smtp** – port 25
- **snmp** – port 161
- **ssl** – port 443
- **telnet** – port 23
- **tftp** – port 69

The **no-health-check** parameter disables the Layer 4 path heath check for this application port. Layer 4 health checks are enabled by default.

To configure the IPv6 firewalls on ServerIron ADX, enter the following commands.

```
ServerIronADX(config)# server fw-name ip6fw1 1112::2
ServerIronADX(config-rs-ip6fw1)# end
ServerIronADX(config)# server fw-name ip6fw2 1112::3
ServerIronADX(config-rs-ip6fw2)# end
ServerIronADX(config)# server fw-group 4 ipv6
ServerIronADX(config-fw-4)# fw-name ip6fw1
ServerIronADX(config-fw-4)# fw-name ip6fw2
```

Syntax: [no] server fw-name *<string> <ipv6-addr>*

Changing the maximum number of sessions

To change the maximum number of sessions the firewall can have on the high-availability pair of
ServerIron ADXs, enter the following command.

```
ServerIronADX(config-rs-FW1)# max-conn 145000
```

Syntax: [no] max-conn *<num>*

The *<num>* variable specifies the maximum and can be from 1 through 2,000,000. This maximum
applies to both the ServerIron ADX and its high-availability partner.

NOTE
Most FWLB parameters, including this one, must be set to the same value on both ServerIron ADXs
in the high-availability pair.

NOTE
If you use the **max-conn** command for a firewall, the command specifies the maximum permissible
number of connections that can be initiated from this ServerIron ADX's direction on the firewall
paths. The **max-conn** command does not limit the total number of connections that can exist on the
ServerIron ADX, which includes connections that come from the ServerIron ADXs at the other ends
of the firewall paths. For FWLB, the command to restrict the total number of connections that can
exist on the ServerIron ADX is **fw-exceed-max-drop**. Refer to "Dropping packets when a firewall
reaches its limit" on page 50.

Connection rate control

Connection rate control enables you to change the maximum number of new TCP or UDP sessions
with the ServerIron ADXs the firewall can have per second.

```
ServerIronADX(config-rs-FW1)# max-tcp-conn-rate 1000
```

Syntax: [no] max-tcp-conn-rate *<num>*

Syntax: [no] max-udp-conn-rate *<num>*

The *<num>* variable specifies the maximum number of connections per second and can be a
number from 1 through 65535. The default is 65535.

Limiting the number of new connections for an application

The following commands limit the rate of new connections per second to TCP port 80 on firewall
FW1.

```
ServerIronADX(config)# server fw-name FW1 1.2.3.4
ServerIronADX(config-rs-FW1)# port http
ServerIronADX(config-rs-FW1)# port http max-tcp-conn-rate 800
```

Syntax: port *<TCP/UDP-portnum>* **max-tcp-conn-rate** *<num>*

Syntax: port *<TCP/UDP-portnum>* **max-udp-conn-rate** *<num>*

The **port** *<TCP/UDP-portnum>* parameter specifies the application port.

The *<num>* variable specifies the maximum number of connections per second.

Adding the firewalls to the firewall group

To add the firewalls to the firewall group, enter the following commands.

```
ServerIronADX(config)# server fw-group-2
ServerIronADX(config-fw-2)# fw-name FW1
ServerIronADX(config-fw-2)# fw-name FW2
```

Syntax: server fw-group 2 | 4

This command changes the CLI to the firewall group configuration level. The IPv4 address format firewall group number is 2. The IPv6 address format firewall group number is 4. These are the only supported firewall groups.

Syntax: [no] fw-name *<string>*

This command adds a configured firewall to the firewall group. For an IPv6 firewall example, refer to "IPv6 example for basic Layer 3 FWLB" on page 24.

Changing the load balancing method

By default, the ServerIron ADX load balances firewall traffic flows by selecting the firewall with the lowest number of total connections. You can configure the ServerIron ADX to load balance based on the lowest number of connections for the traffic flow's application.

For example, suppose a configuration has two firewalls (FW1 and FW2), and each firewall has two application ports defined (HTTP and SMTP). Also assume the following:

- FW1 has 10 HTTP connections and 80 SMTP connections.
- FW2 has 60 HTTP connections and 10 SMTP connections.

Using the default load balancing method, traffic for a new flow is load balanced to FW2, because this firewall has fewer total connections. This is true regardless of the application in the traffic. However, using the load balancing by application method, a new traffic flow carrying HTTP traffic is load balanced to FW1 instead of FW2, because FW1 has fewer HTTP connections. A new traffic flow for SMTP is load balanced to FW2, because FW2 has fewer SMTP connections.

To enable load balancing by application, enter the following command at the firewall group configuration level.

```
ServerIronADX(config-fw-2)# fw-predictor per-service-least-conn
```

Syntax: [no] fw-predictor total-least-conn | per-service-least-conn

The **total-least-conn** parameter load balances traffic based on the total number of connections only. This is the default.

The **per-service-least-conn** parameter load balances traffic based on the total number of connections for the traffic's application. This is valid for TCP or UDP applications.

Hashing load balance metric in FWLB

You configure the **fw-predictor hash** command under the firewall group. When this command is configured, firewall selection is based on hashing of IP addresses (and ports optionally). The packet will be dropped if hashing picks a firewall and if either of the following is true:

- The maximum number of sessions (**max-conn** command) is reached for that firewall.
- The connection rate is exceeded for the firewall or the firewall port.

    The connection rate can be specified at the firewall level or a firewall port level.

To configure the hashing features, enter the following commands.

```
SLB-SI-A(config)# server fw-group 2
SLB-SI-A(config-fw-2)# fw-predictor hash
```

Syntax: **fw-predictor hash**

Enabling the active-active mode

To enable the FWLB active-active mode, enter a command such as the following at the firewall group configuration level.

```
ServerIronADX(config-fw-2)# sym-priority 1
```

Syntax: **[no] sym-priority** *<num>*

The **sym-priority** command enables the active-active mode.

The *<num>* variable specifies a priority value from 1 through 255. While a value must be used, it does not affect operation of the ServerIron ADX.

Using the value of "0" for the *<num>* variable is a special case. If you specify "0", the CLI removes the priority. When you save the configuration to the startup-config file, the **sym-priority** command is removed. You cannot remove the priority using the **no sym-priority** command.

This command is also used for Symmetric Server Load Balancing (SSLB) where the value of the *<num>* variable is significant. For more information about SSLB see the "Symmetric SLB" section of the "High Availability" chapter in the *ServerIron ADX Server Load Balancing Guide*.

Configuring the paths and static MAC address entries

The paths go from one ServerIron ADX to the other ServerIron ADXs on the other side of each firewall. A path also goes to the router.

A path consists of the following parameters:

- The path ID – A number that identifies the path. The paths go from one ServerIron ADX to the other through the firewalls. A path also goes to the router. On each ServerIron ADX, the sequence of path IDs must be contiguous (with no gaps), starting with path ID 1. For example, path sequence 1, 2, 3, 4, 5 is valid. Path sequence 1, 3, 5 or 5, 4, 3, 2, 1 is not valid.
- The ServerIron ADX port – The number of the port that connects the ServerIron ADX to the firewall. If your configuration does not require static MAC entries, you can specify a dynamic port (65535) instead of the physical port number for firewall paths. Specifying the dynamic port allows the ServerIron ADX to select the physical port for the path so you do not need to do so. You cannot specify the dynamic port for router paths. Router paths require the physical port number.

- The other ServerIron ADX's IP address – The management address of the ServerIron ADX on the other side of the firewall.

- The next-hop IP address – The IP address of the firewall interface connected to this ServerIron ADX.

NOTE
FWLB paths must be fully meshed. When you configure a FWLB path on a ServerIron ADX, make sure you also configure a reciprocal path on the ServerIron ADX attached to the other end of the firewalls. For example, if you configure four paths to four separate firewalls, make sure you configure four paths on the other ServerIron ADX.

NOTE
In addition to configuring the paths, some configurations require a static MAC entry for each firewall interface attached to the ServerIron ADX. Each configuration example in this guide indicates whether the configuration requires static MAC entries. The static MAC entries are not required if the routers are using OSPF.

To configure paths for ServerIron ADX SI-Ext-A in Figure 10 on page 40, enter the following commands.

```
ServerIronADX(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
ServerIronADX(config-fw-2)# fwall-info 2 4/5 10.10.2.222 10.10.1.2
ServerIronADX(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
ServerIronADX(config-fw-2)# fwall-info 4 4/5 10.10.2.223 10.10.1.2
ServerIronADX(config-fw-2)# fwall-info 5 4/12 10.10.1.101 10.10.1.101
```

Syntax: (IPv4) [no] fwall-info *<path-num> <portnum> <other-ip> <next-hop-ip>*

Syntax: (IPv6) [no] fwall-info *<path-num> <portnum> <other-ipv6> <next-hop-ipv6>*

NOTE
The other IP address and next-hop IP address parameters must be both IPv4 addresses or both IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

NOTE
You must use IPv4 addresses for IPv4 firewalls and IPv6 addresses for IPv6 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

The *<path-num>* parameter specifies the path. The sequence of path IDs must be contiguous from start to finish.

The *<portnum>* parameter specifies the port that connects the ServerIron ADX to the firewall. If the port number is dynamic, use port number 65535.

The *<other-ip>* parameter specifies the IPv4 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ip>* parameter specifies the IPv4 address of the firewall connected to this ServerIron ADX.

The *<other-ipv6>* parameter specifies the IPv6 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ipv6>* parameter specifies the IPv6 address of the firewall connected to this ServerIron ADX.

To configure the static MAC address entries for ServerIron ADX SI-Ext-A in Figure 10, enter the following commands.

```
ServerIronADX(config-fw-2)# vlan 1
ServerIronADX(config-vlan-1)# static-mac-address 0050.da92.08fc ethernet 4/5
priority 1 router-type
ServerIronADX(config-vlan-1)# static-mac-address 0050.da8d.5218 ethernet 4/1
priority 1 router-type
```

Syntax: [no] static-mac-address *<mac-addr>* ethernet *<portnum>* [priority *<0-7>*] [host-type | router-type]

The priority can be from 0 through 7 (0 is lowest and 7 is highest). Use a priority higher than 0.

Use router-type for the entry type.

If you are using the always-active feature (by entering the always-active command in VLAN 1 for simplified Layer 2 topology), you also must enable the L2-Fwall feature by entering the following command.

```
ServerIronADX(config-fw-2)# l2-fwall
```

Syntax: [no] l2-fwall

Dropping packets when a firewall reaches its limit

By default, if the ServerIron ADX receives traffic that it needs to forward to a firewall, but the firewall already has the maximum number of sessions open or has exceeded its maximum connection rate, the ServerIron ADX uses a hashing mechanism to select another firewall. The hashing mechanism selects another firewall based on the source and destination IP addresses and application port numbers in the packet.

If you want the ServerIron ADX to drop the traffic instead of load balancing it using the hashing mechanism, enter the following command.

```
ServerIronADX(config-fw-2)# fw-exceed-max-drop
```

Syntax: [no] fw-exceed-max-drop

The ServerIron ADX drops traffic only until the firewall again has available sessions.

Restricting TCP traffic to a firewall to established sessions

By default, the ServerIron ADX sends a properly addressed TCP data packet to a firewall regardless of whether the ServerIron ADX has received a TCP SYN for the traffic flow. For example, if the ServerIron ADX receives a TCP packet addressed to TCP port 8080 on IP address 1.1.1.1, the ServerIron ADX forwards the packet to the firewall connected to 1.1.1.1 regardless of whether the ServerIron ADX has received a TCP SYN for the session between the packet's source and 1.1.1.1.

For tighter security, you can configure the ServerIron ADX to forward a TCP data packet only if the ServerIron ADX has already received a TCP SYN for the packet's traffic flow (source and destination addresses). For example, with the tighter security enabled, the ServerIron ADX does not forward a TCP data packet to 1.1.1.1 unless the ServerIron ADX has already received a TCP SYN for the session between the packet's source and 1.1.1.1.

To enable the tighter security, enter the following command at the global CONFIG level of the CLI.

```
ServerIronADX(config)# server fw-strict-sec
```

Syntax: [no] server fw-strict-sec

The feature applies globally to all TCP traffic received for FWLB.

Complete CLI example

The following sections show the CLI commands for configuring the ServerIron ADXs in Figure 10.

Commands on ServerIron ADX SI-Ext-A

The following commands add a management IP address and default gateway address to the ServerIron ADX. The IP address must be in the same sub-net as the ServerIron ADX's interfaces with the Layer 3 firewalls.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-A
SI-Ext-A(config)# ip address 10.10.1.111 255.255.255.0
SI-Ext-A(config)# ip default-gateway 10.10.1.101
```

The following commands configure trunk groups for the synchronization link and the additional data link between this ServerIron ADX and its high-availability partner.

```
SI-Ext-A(config)# trunk switch ethernet 4/5 to 4/6
SI-Ext-A(config)# trunk deploy
SI-Ext-A(config)# trunk switch ethernet 4/13 to 4/14
SI-Ext-A(config)# trunk deploy
```

The following commands enable the always-active feature and disable the Spanning Tree Protocol (STP) in VLAN 1, which contains the ports that will carry the FWLB traffic.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# always-active
SI-Ext-A(config-vlan-1)# no spanning-tree
SI-Ext-A(config-vlan-1)# exit
```

The following commands configure the ports for the synchronization link to the other ServerIron ADX in a separate port-based VLAN. The separate VLAN is required. Add the ports as untagged ports.

```
SI-Ext-A(config)# vlan 2 name sync_link by port
SI-Ext-A(config-vlan-2)# untagged ethernet 4/13 to 4/14
SI-Ext-A(config-vlan-2)# no spanning-tree
SI-Ext-A(config-vlan-2)# exit
```

The **server fw-port** command identifies the port that connects this ServerIron ADX to its high-availability partner. The **server partner-ports** command identifies the data link that connects this ServerIron ADX to its high-availability partner to reach the firewalls. If you use a trunk group, specify the first port in the group (the group's primary port).

```
SI-Ext-A(config)# server fw-port 4/13
SI-Ext-A(config)# server partner-ports ethernet 4/5
```

The **server router-port** command identifies the port that connects this ServerIron ADX to its default gateway router.

```
SI-Ext-A(config)# server router-port 4/12
```

The following commands configure the firewalls and add them to the firewall group. Because an application port is configured on each firewall, the ServerIron ADX will use Layer 4 sessions to load balance the firewall traffic for that application. The ServerIron ADX will use Layer 3 sessions to load balance traffic for other applications.

```
SI-Ext-A(config)# server fw-name FW1 10.10.1.1
SI-Ext-A(config-rs-FW1)# port http
SI-Ext-A(config-rs-FW1)# exit
SI-Ext-A(config)# server fw-name FW2 10.10.1.2
SI-Ext-A(config-rs-FW2)# port http
SI-Ext-A(config-rs-FW2)# server fw-group 2
SI-Ext-A(config-fw-2)# fw-name FW1
SI-Ext-A(config-fw-2)# fw-name FW2
```

The following command enables the active-active mode. The CLI requires a number from 1 through 255. See "Enabling the active-active mode" on page 48 for more details.

```
SI-Ext-A(config-fw-2)# sym-priority 1
```

The following commands configure the data paths through the firewalls and to the default gateway router. The **l2-fwall** command is part of the always-active feature and is required if you use the **always-active** command.

```
SI-Ext-A(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 2 4/5 10.10.2.222 10.10.1.2
SI-Ext-A(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 4 4/5 10.10.2.223 10.10.1.2
SI-Ext-A(config-fw-2)# fwall-info 5 4/12 10.10.1.101 10.10.1.101
SI-Ext-A(config-fw-2)# l2-fwall
SI-Ext-A(config-fw-2)# exit
```

The following commands add static entries to the ServerIron ADX's MAC table for the firewall interfaces. Specify a priority higher than 0. You can specify a priority up to 7. The **router-type** parameter is required for FWLB.

The following commands also enable FWLB and save the configuration changes to the startup-config file.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# static-mac-address 0050.da8d.5218 ethernet 4/1 priority
1
router-type
SI-Ext-A(config-vlan-1)# static-mac-address 0050.da92.08fc ethernet 4/5 priority
1
router-type
SI-Ext-A(config-vlan-1)# exit
SI-Ext-A(config)# write memory
```

Commands on ServerIron ADX SI-Ext-B

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-B
SI-Ext-B(config)# ip address 10.10.1.112 255.255.255.0
SI-Ext-B(config)# ip default-gateway 10.10.1.101
SI-Ext-B(config)# trunk switch ethernet 4/5 to 4/6
SI-Ext-B(config)# trunk deploy
SI-Ext-B(config)# trunk switch ethernet 4/13 to 4/14
SI-Ext-B(config)# trunk deploy
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# always-active
SI-Ext-B(config-vlan-1)# no spanning-tree
SI-Ext-B(config-vlan-1)# exit
SI-Ext-B(config)# vlan 2 name sync_link by port
SI-Ext-B(config-vlan-2)# untagged ethernet 4/13 to 4/14
SI-Ext-B(config-vlan-2)# no spanning-tree
SI-Ext-B(config-vlan-2)# exit
SI-Ext-B(config)# server fw-port 4/13
SI-Ext-B(config)# server router-ports 4/12
SI-Ext-B(config)# server fw-name FW1 10.10.1.1
SI-Ext-B(config-rs-FW1)# port http
SI-Ext-B(config-rs-FW1)# exit
SI-Ext-B(config)# server fw-name FW2 10.10.1.2
SI-Ext-B(config-rs-FW2)# port http
SI-Ext-B(config-rs-FW2)# server fw-group 2
SI-Ext-B(config-fw-2)# fw-name FW1
SI-Ext-B(config-fw-2)# fw-name FW2
SI-Ext-B(config-fw-2)# sym-priority 1
SI-Ext-B(config-fw-2)# fwall-info 1 4/5 10.10.2.222 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 2 4/1 10.10.2.222 10.10.1.2
SI-Ext-B(config-fw-2)# fwall-info 3 4/5 10.10.2.223 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 4 4/1 10.10.2.223 10.10.1.2
SI-Ext-B(config-fw-2)# fwall-info 5 4/12 10.10.1.101 10.10.1.101
SI-Ext-B(config-fw-2)# l2-fwall
SI-Ext-B(config-fw-2)# exit
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# static-mac-address 0050.da8d.5218 ethernet 4/5 priority
1
router-type
SI-Ext-B(config-vlan-1)# static-mac-address 0050.da92.08fc ethernet 4/1 priority
1
router-type
SI-Ext-B(config-vlan-1)# exit
SI-Ext-B(config)# write memory
SI-Ext-B(config)# end
```

Commands on ServerIron ADX SI-Int-A

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-A
SI-Int-A(config)# ip address 10.10.2.222 255.255.255.0
SI-Int-A(config)# ip default-gateway 10.10.2.101
SI-Int-A(config)# trunk switch ethernet 4/5 to 4/6
SI-Int-A(config)# trunk deploy
SI-Int-A(config)# trunk switch ethernet 4/13 to 4/14
SI-Int-A(config)# trunk deploy
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# always-active
SI-Int-A(config-vlan-1)# no spanning-tree
SI-Int-A(config-vlan-1)# exit
SI-Int-A(config)# vlan 2 name sync_link by port
SI-Int-A(config-vlan-2)# untagged ethernet 4/13 to 4/14
SI-Int-A(config-vlan-2)# no spanning-tree
SI-Int-A(config-vlan-2)# exit
SI-Int-A(config)# server fw-port 4/13
SI-Ext-A(config)# server partner-ports ethernet 4/5
SI-Int-A(config)# server router-ports 4/12
SI-Int-A(config)# server fw-name FW1 10.10.2.1
SI-Int-A(config-rs-FW1)# port http
SI-Int-A(config-rs-FW1)# exit
SI-Int-A(config)# server fw-name FW2 10.10.2.2
SI-Int-A(config-rs-FW2)# port http
SI-Int-A(config-rs-FW2)# server fw-group 2
SI-Int-A(config-fw-2)# fw-name FW1
SI-Int-A(config-fw-2)# fw-name FW2
SI-Int-A(config-fw-2)# sym-priority 1
SI-Int-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 2 4/5 10.10.1.111 10.10.2.2
SI-Int-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 4 4/5 10.10.1.112 10.10.2.2
SI-Int-A(config-fw-2)# fwall-info 5 4/12 10.10.2.101 10.10.2.101
SI-Int-A(config-fw-2)# l2-fwall
SI-Int-A(config-fw-2)# exit
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# static-mac-address 0050.da92.08dc ethernet 4/1 priority
1
router-type
SI-Int-A(config-vlan-1)# static-mac-address 0050.da92.08d0 ethernet 4/5 priority
1
router-type
SI-Int-A(config-vlan-1)# exit
SI-Int-A(config)# write memory
SI-Int-A(config)# end
```

Commands on ServerIron ADX SI-Int-B

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-B
SI-Int-B(config)# ip address 10.10.2.223 255.255.255.0
SI-Int-B(config)# ip default-gateway 10.10.2.101
SI-Int-B(config)# trunk switch ethernet 4/5 to 4/6
SI-Int-B(config)# trunk deploy
SI-Int-B(config)# trunk switch ethernet 4/13 to 4/14
SI-Int-B(config)# trunk deploy
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# always-active
SI-Int-B(config-vlan-1)# no spanning-tree
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# vlan 2 name sync_link by port
SI-Int-B(config-vlan-2)# untagged ethernet 4/13 to 4/14
SI-Int-B(config-vlan-2)# no spanning-tree
SI-Int-B(config-vlan-2)# exit
SI-Int-B(config)# server fw-port 4/13
SI-Int-B(config)# server router-ports 4/12
SI-Int-B(config)# server fw-name FW1 10.10.2.1
SI-Int-B(config-rs-FW1)# port http
SI-Int-B(config-rs-FW1)# exit
SI-Int-B(config)# server fw-name FW2 10.10.2.2
SI-Int-B(config-rs-FW2)# port http
SI-Int-B(config-rs-FW2)# server fw-group 2
SI-Int-B(config-fw-2)# fw-name FW1
SI-Int-B(config-fw-2)# fw-name FW2
SI-Int-B(config-fw-2)# sym-priority 1
SI-Int-B(config-fw-2)# fwall-info 1 4/5 10.10.1.111 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 2 4/1 10.10.1.111 10.10.2.2
SI-Int-B(config-fw-2)# fwall-info 3 4/5 10.10.1.112 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 4 4/1 10.10.1.112 10.10.2.2
SI-Int-B(config-fw-2)# fwall-info 5 4/12 10.10.2.101 10.10.2.101
SI-Int-B(config-fw-2)# l2-fwall
SI-Int-B(config-fw-2)# exit
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# static-mac-address 0050.da92.08dc ethernet 4/5 priority
1
router-type
SI-Int-B(config-vlan-1)# static-mac-address 0050.da92.08d0 ethernet 4/1 priority
1
router-type
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# write memory
SI-Int-B(config)# end
```

Configuring active-active HA FWLB

The following configuration and diagram is example of active-active FWLB.

FIGURE 11   Active-active FWLB topology
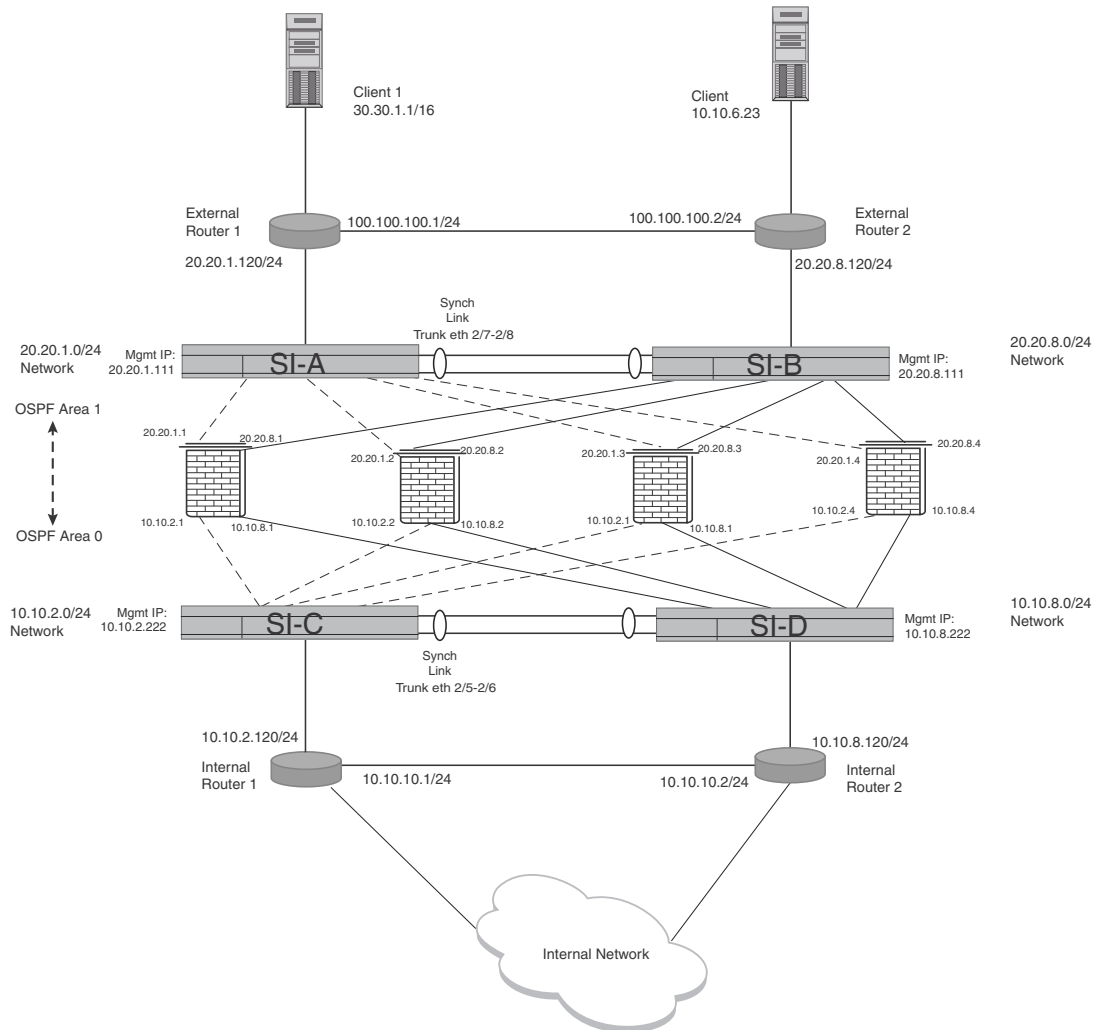
Notes about the configuration:

- FWLB ServerIron ADXs work in active-active mode. Firewall paths will be up on both the ServerIron ADXs and both ServerIron ADXs can do FWLB.

- The **always-active** command is configured under VLAN 1. This command should not be configured under **synch ports vlan**.

- Stateful algorithm is used for FWLB; therefore, the ServerIron ADX needs to synchronize sessions with its partner ServerIron ADX to support stateful failover in high availability FWLB configurations.

- In the topology presented in this section, IP addresses of firewalls are different on each ServerIron ADX. Use the **other-ip** command under the firewall configuration level to identify the partner ServerIron ADX's firewall address.

  Syntax: [no] other-ip *<ip-addr>* | *<ipv6-addr>*

  NOTE
  IPv4 and IPv6 address formats cannot be mixed. Addresses must be entered in the same format.

- This topology assumes that OSPF is running on firewalls, external routers, and internal routers. These devices exchange OSPF messages (multicast packets) among them. When a ServerIron ADX is in state 3, it will block multicast packets. In the attached topology, if Ext-SI-B is in state 3, it will block the OSPF multicast packets sent by the firewalls and Ext-Router-2 to prevent Ext-Router-2 and the firewalls from learning OSPF routes through each other. Ext-Router-2 learns the OSPF routes of internal networks through Ext-Router-1. All the external traffic will be going to Ext-SI-A.

- If the design requires ServerIron ADX (in state 3) not to block multicast packets, the **server fw-allow-multicast** command must be configured on the ServerIron ADXs. When the command is configured, the external routers can learn the OSPF routes from the firewalls and traffic can go to both ServerIron ADXs.

Note that the following example uses the IPv4 address format and firewall group 2.

External ServerIron ADX standby A (Ext-SI-A) configuration

```
SI-StandbyA(config)# trunk switch ethernet 2/7 to 2/8
SI-StandbyA(config)# server fw-port 2/7
SI-StandbyA(config)# server partner-ports ethernet 4/5
SI-StandbyA(config)# server router-ports ethernet 2/1
SI-StandbyA(config)# server fw-name fw1 20.20.1.1
SI-StandbyA(config-rs-FW1)# other-ip 20.20.8.1
SI-StandbyA(config-rs-FW1)# port http
SI-StandbyA(config-rs-FW1)# port http no-health-check
SI-StandbyA(config-rs-FW1)# port http url "HEAD /"
SI-StandbyA(config-rs-FW1)# exit
SI-StandbyA(config)# server fw-name fw2 20.20.1.2
SI-StandbyA(config-rs-FW2)# other-ip 20.20.8.2
SI-StandbyA(config-rs-FW2)# port http
SI-StandbyA(config-rs-FW2)# port http no-health-check
SI-StandbyA(config-rs-FW2)# port http url "HEAD /"
SI-StandbyA(config-rs-FW2)# exit
SI-StandbyA(config)# server fw-name fw3 20.20.1.3
SI-StandbyA(config-rs-FW3)# other-ip 20.20.8.3
SI-StandbyA(config-rs-FW3)# port http
SI-StandbyA(config-rs-FW3)# port http no-health-check
SI-StandbyA(config-rs-FW3)# port http url "HEAD /"
SI-StandbyA(config-rs-FW3)# exit
SI-StandbyA(config)# server fw-name fw4 20.20.1.4
SI-StandbyA(config-rs-FW4)# other-ip 20.20.8.4
SI-StandbyA(config-rs-FW4)# port http
SI-StandbyA(config-rs-FW4)# port http no-health-check
SI-StandbyA(config-rs-FW4)# port http url "HEAD /"
```

```
SI-StandbyA(config-rs-FW4)# server fw-group 2
SI-StandbyA(config-fw-2)# l2-fwall
SI-StandbyA(config-fw-2)# sym-priority 250
SI-StandbyA(config-fw-2)# fw-name fw1
SI-StandbyA(config-fw-2)# fw-name fw2
SI-StandbyA(config-fw-2)# fw-name fw3
SI-StandbyA(config-fw-2)# fw-name fw4
SI-StandbyA(config-fw-2)# fwall-info 1 3/1 10.10.2.222 20.20.1.1
SI-StandbyA(config-fw-2)# fwall-info 2 3/2 10.10.2.222 20.20.1.2
SI-StandbyA(config-fw-2)# fwall-info 3 3/3 10.10.2.222 20.20.1.3
SI-StandbyA(config-fw-2)# fwall-info 4 3/4 10.10.2.222 20.20.1.4
SI-StandbyA(config-fw-2)# fwall-info 5 3/1 10.10.8.222 20.20.1.1
SI-StandbyA(config-fw-2)# fwall-info 6 3/2 10.10.8.222 20.20.1.2
SI-StandbyA(config-fw-2)# fwall-info 7 3/3 10.10.8.222 20.20.1.3
SI-StandbyA(config-fw-2)# fwall-info 8 3/4 10.10.8.222 20.20.1.4
SI-StandbyA(config-fw-2)# fwall-info 9 2/1 20.20.1.120 20.20.1.120
SI-StandbyA(config-fw-2)# fw-predictor per-service-least-conn
SI-StandbyA(config-fw-2)# exit
SI-StandbyA(config)# vlan 1 name DEFAULT-VLAN by port
SI-StandbyA(config-vlan-1)# always-active
SI-StandbyA(config-vlan-1)# no spanning-tree
SI-StandbyA(config-vlan-1)# static-mac-address 0004.80ed.17b4 ethernet 3/1
priority 1 router-type
SI-StandbyA(config-vlan-1)# static-mac-address 0004.80f0.4b3c ethernet 3/2
priority 1 router-type
SI-StandbyA(config-vlan-1)# static-mac-address 0004.80ed.1368 ethernet 3/3
priority 1 router-type
SI-StandbyA(config-vlan-1)# static-mac-address 0004.80eb.5294 ethernet 3/4
priority 1 router-type
SI-StandbyA(config-vlan-1)# exit
SI-StandbyA(config)# vlan 999 by port
SI-StandbyA(config-vlan-999)# untagged ethernet 2/7 to 2/8
SI-StandbyA(config-vlan-999)# no spanning-tree
SI-StandbyA(config-vlan-999)# exit
SI-StandbyA(config)# hostname Ext-SI-A
SI-StandbyA(config)# ip address 20.20.1.111 255.255.255.0
SI-StandbyA(config)# ip default-gateway 20.20.1.120
SI-StandbyA(config)# write memory
SI-StandbyA(config)# end
SI-StandbyA(config)# reload
```

External ServerIron ADX standby B (Ext-SI-B) configuration

```
SI-StandbyB(config)# trunk switch ethernet 2/7 to 2/8
SI-StandbyB(config)# server fw-port 2/7
SI-StandbyB(config)# server partner-ports ethernet 4/5
SI-StandbyB(config)# server router-ports ethernet 2/1
SI-StandbyB(config)# server fw-name fw1 20.20.8.1
SI-StandbyB(config-rs-FW1)# other-ip 20.20.1.1
SI-StandbyB(config-rs-FW1)# port http
SI-StandbyB(config-rs-FW1)# port http no-health-check
SI-StandbyB(config-rs-FW1)# port http url "HEAD /"
SI-StandbyB(config-rs-FW1)# exit
```

```
SI-StandbyB(config)#server fw-name fw2 20.20.8.2
SI-StandbyB(config-rs-FW2)# other-ip 20.20.1.2
SI-StandbyB(config-rs-FW2)# port http
SI-StandbyB(config-rs-FW2)# port http no-health-check
SI-StandbyB(config-rs-FW2)# port http url "HEAD /"
SI-StandbyB(config-rs-FW2)# exit
SI-StandbyB(config)# server fw-name fw3 20.20.8.3
SI-StandbyB(config-rs-FW3)# other-ip 20.20.1.3
SI-StandbyB(config-rs-FW3)# port http
SI-StandbyB(config-rs-FW3)# port http no-health-check
SI-StandbyB(config-rs-FW3)# port http url "HEAD /"
SI-StandbyB(config-rs-FW3)# exit
SI-StandbyB(config)# server fw-name fw4 20.20.8.4
SI-StandbyB(config-rs-FW4)# other-ip 20.20.1.4
SI-StandbyB(config-rs-FW4)# port http
SI-StandbyB(config-rs-FW4)# port http no-health-check
SI-StandbyB(config-rs-FW4)# port http url "HEAD /"
SI-StandbyB(config-rs-FW4)# exit
SI-StandbyB(config-rs-FW4)# server fw-group 2
SI-StandbyB(config-rs-tc-2)# l2-fwall
SI-StandbyB(config-rs-tc-2)# sym-priority 10
SI-StandbyB(config-rs-tc-2)# fw-name fw1
SI-StandbyB(config-rs-tc-2)# fw-name fw2
SI-StandbyB(config-rs-tc-2)# fw-name fw3
SI-StandbyB(config-rs-tc-2)# fw-name fw4
SI-StandbyB(config-rs-tc-2)# fwall-info 1 3/1 10.10.8.222 20.20.8.1
SI-StandbyB(config-rs-tc-2)# fwall-info 2 3/2 10.10.8.222 20.20.8.2
SI-StandbyB(config-rs-tc-2)# fwall-info 3 3/3 10.10.8.222 20.20.8.3
SI-StandbyB(config-rs-tc-2)# fwall-info 4 3/4 10.10.8.222 20.20.8.4
SI-StandbyB(config-rs-tc-2)# fwall-info 5 3/1 10.10.2.222 20.20.8.1
SI-StandbyB(config-rs-tc-2)# fwall-info 6 3/2 10.10.2.222 20.20.8.2
SI-StandbyB(config-rs-tc-2)# fwall-info 7 3/3 10.10.2.222 20.20.8.3
SI-StandbyB(config-rs-tc-2)# fwall-info 8 3/4 10.10.2.222 20.20.8.4
SI-StandbyB(config-rs-tc-2)# fwall-info 9 2/1 20.20.8.120 20.20.8.120
SI-StandbyB(config-rs-tc-2)# fw-predictor per-service-least-conn
SI-StandbyB(config-rs-tc-2)# exit
SI-StandbyB(config)# vlan 1 name DEFAULT-VLAN by port
SI-StandbyB(config-vlan-1)# always-active
SI-StandbyB(config-vlan-1)# no spanning-tree
SI-StandbyB(config-vlan-1)# static-mac-address 0004.80ed.17b4 ethernet 3/1
priority 1 router-type
SI-StandbyB(config-vlan-1)# static-mac-address 0004.80f0.4b3c ethernet 3/2
priority 1 router-type
SI-StandbyB(config-vlan-1)# static-mac-address 0004.80ed.1368 ethernet 3/3
priority 1 router-type
SI-StandbyB(config-vlan-1)# static-mac-address 0004.80eb.5294 ethernet 3/4
priority 1 router-type
SI-StandbyB(config-vlan-1)# exit
SI-StandbyB(config)# vlan 999 by port
SI-StandbyB(config-vlan-999)# untagged ethe 2/7 to 2/8
SI-StandbyB(config-vlan-999)# no spanning-tree
SI-StandbyB(config-vlan-999)# exit
SI-StandbyB(config)# hostname Ext-SI-B
SI-StandbyB(config)# ip address 20.20.8.111 255.255.255.0
SI-StandbyB(config)# ip default-gateway 20.20.8.120
SI-StandbyB(config)# write memory
SI-StandbyB(config)# end
SI-StandbyB(config)# reload
```

Internal ServerIron ADX C (Int-SI-C) Configuration

```
SI-ActiveC(config)# trunk switch ethe 2/5 to 2/6
SI-ActiveC(config)# server fw-port 2/5
SI-ActiveC(config)# server partner-ports ethernet 4/5
SI-ActiveC(config)# server router-ports ethernet 2/1
SI-ActiveC(config)# server fw-name fw1 10.10.2.1
SI-ActiveC(config-rs-FW1)# other-ip 10.10.8.1
SI-ActiveC(config-rs-FW1)# port http
SI-ActiveC(config-rs-FW1)# port http no-health-check
SI-ActiveC(config-rs-FW1)# port http url "HEAD /"
SI-ActiveC(config-rs-FW1)# exit
SI-ActiveC(config)# server fw-name fw2 10.10.2.2
SI-ActiveC(config-rs-FW2)# other-ip 10.10.8.2
SI-ActiveC(config-rs-FW2)# port http
SI-ActiveC(config-rs-FW2)# port http no-health-check
SI-ActiveC(config-rs-FW2)# port http url "HEAD /"
SI-ActiveC(config-rs-FW2)# exit
SI-ActiveC(config)# server fw-name fw3 10.10.2.3
SI-ActiveC(config-rs-FW3)# other-ip 10.10.8.3
SI-ActiveC(config-rs-FW3)# port http
SI-ActiveC(config-rs-FW3)# port http no-health-check
SI-ActiveC(config-rs-FW3)# port http url "HEAD /"
SI-ActiveC(config-rs-FW3)# exit
SI-ActiveC(config)# server fw-name fw4 10.10.2.4
SI-ActiveC(config-rs-FW4)# other-ip 10.10.8.4
SI-ActiveC(config-rs-FW4)# port http
SI-ActiveC(config-rs-FW4)# port http no-health-check
SI-ActiveC(config-rs-FW4)# port http url "HEAD /"
SI-ActiveC(config-rs-FW4)# exit
SI-ActiveC(config-rs-FW4)# server fw-group 2
SI-ActiveC(config-fw-2)# l2-fwall
SI-ActiveC(config-fw-2)# sym-priority 250
SI-ActiveC(config-fw-2)# fw-name fw1
SI-ActiveC(config-fw-2)# fw-name fw2
SI-ActiveC(config-fw-2)# fw-name fw3
SI-ActiveC(config-fw-2)# fw-name fw4
SI-ActiveC(config-fw-2)# fwall-info 1 3/1 20.20.1.111 10.10.2.1
SI-ActiveC(config-fw-2)# fwall-info 2 3/2 20.20.1.111 10.10.2.2
SI-ActiveC(config-fw-2)# fwall-info 3 3/3 20.20.1.111 10.10.2.3
SI-ActiveC(config-fw-2)# fwall-info 4 3/4 20.20.1.111 10.10.2.4
SI-ActiveC(config-fw-2)# fwall-info 5 3/1 20.20.8.111 10.10.2.1
SI-ActiveC(config-fw-2)# fwall-info 6 3/2 20.20.8.111 10.10.2.2
SI-ActiveC(config-fw-2)# fwall-info 7 3/3 20.20.8.111 10.10.2.3
SI-ActiveC(config-fw-2)# fwall-info 8 3/4 20.20.8.111 10.10.2.4
SI-ActiveC(config-fw-2)# fwall-info 9 2/1 10.10.2.120 10.10.2.120
SI-ActiveC(config-fw-2)# fw-predictor per-service-least-conn
SI-ActiveC(config-fw-2)# exit
SI-ActiveC(config)# vlan 1 name DEFAULT-VLAN by port
SI-ActiveC(config-vlan-1)# always-active
SI-ActiveC(config-vlan-1)# no spanning-tree
SI-ActiveC(config-vlan-1)# static-mac-address 0004.80ed.17b4 ethernet 3/1
priority 1 router-type
SI-ActiveC(config-vlan-1)# static-mac-address 0004.80f0.4b3c ethernet 3/2
priority 1 router-type
SI-ActiveC(config-vlan-1)# static-mac-address 0004.80ed.1368 ethernet 3/3
```

```
priority 1 router-type
SI-ActiveC(config-vlan-1)# static-mac-address 0004.80eb.5294 ethernet 3/4
priority 1 router-type
SI-ActiveC(config-vlan-1)# exit
SI-ActiveC(config)# vlan 999 by port
SI-ActiveC(config-vlan-999)# untagged ethe 2/5 to 2/8
SI-ActiveC(config-vlan-999)# no spanning-tree
SI-ActiveC(config-vlan-999)# exit
SI-ActiveC(config)# hostname Int-SI-C
SI-ActiveC(config)# ip address 10.10.2.222 255.255.255.0
SI-ActiveC(config)# ip default-gateway 10.10.2.120
SI-ActiveC(config)# write mem
SI-ActiveC(config)# end
SI-ActiveC(config)# reload
```

Internal ServerIron ADX D (Int-SI-D) configuration

```
SI-ActiveD(config)# trunk switch ethe 2/5 to 2/6
SI-ActiveD(config)# server fw-port 2/5
SI-ActiveD(config)# server partner-ports ethernet 4/5
SI-ActiveD(config)# server router-ports ethernet 2/1
SI-ActiveD(config)# server fw-name fw1 10.10.8.1
SI-ActiveD(config-rs-FW1)# other-ip 10.10.2.1
SI-ActiveD(config-rs-FW1)# port http
SI-ActiveD(config-rs-FW1)# port http no-health-check
SI-ActiveD(config-rs-FW1)# port http url "HEAD /"
SI-ActiveD(config-rs-FW1)# exit
SI-ActiveD(config)# server fw-name fw2 10.10.8.2
SI-ActiveD(config-rs-FW2)# other-ip 10.10.2.2
SI-ActiveD(config-rs-FW2)# port http
SI-ActiveD(config-rs-FW2)# port http no-health-check
SI-ActiveD(config-rs-FW2)# port http url "HEAD /"
SI-ActiveD(config-rs-FW2)# exit
SI-ActiveD(config)# server fw-name fw3 10.10.8.3
SI-ActiveD(config-rs-FW3)# other-ip 10.10.2.3
SI-ActiveD(config-rs-FW3)# port http
SI-ActiveD(config-rs-FW3)# port http no-health-check
SI-ActiveD(config-rs-FW3)# port http url "HEAD /"
SI-ActiveD(config-rs-FW3)#
SI-ActiveD(config)# server fw-name fw4 10.10.8.4
SI-ActiveD(config-rs-FW4)# other-ip 10.10.2.4
SI-ActiveD(config-rs-FW4)# port http
SI-ActiveD(config-rs-FW4)# port http no-health-check
SI-ActiveD(config-rs-FW4)# port http url "HEAD /"
SI-ActiveD(config-rs-FW4)# exit
SI-ActiveD(config-rs-FW4)# server fw-group 2
SI-ActiveD(config-fw-2)# l2-fwall
SI-ActiveD(config-fw-2)# sym-priority 10
SI-ActiveD(config-fw-2)# fw-name fw1
SI-ActiveD(config-fw-2)# fw-name fw2
SI-ActiveD(config-fw-2)# fw-name fw3
SI-ActiveD(config-fw-2)# fw-name fw4
SI-ActiveD(config-fw-2)# fwall-info 1 3/1 20.20.8.111 10.10.8.1
SI-ActiveD(config-fw-2)# fwall-info 2 3/2 20.20.8.111 10.10.8.2
SI-ActiveD(config-fw-2)# fwall-info 3 3/3 20.20.8.111 10.10.8.3
SI-ActiveD(config-fw-2)# fwall-info 4 3/4 20.20.8.111 10.10.8.4
SI-ActiveD(config-fw-2)# fwall-info 5 3/1 20.20.1.111 10.10.8.1
SI-ActiveD(config-fw-2)# fwall-info 6 3/2 20.20.1.111 10.10.8.2
```

```
SI-ActiveD(config-fw-2)# fwall-info 7 3/3 20.20.1.111 10.10.8.3
SI-ActiveD(config-fw-2)# fwall-info 8 3/4 20.20.1.111 10.10.8.4
SI-ActiveD(config-fw-2)# fwall-info 9 2/1 10.10.8.120 10.10.8.120
SI-ActiveD(config-fw-2)# fw-predictor per-service-least-conn
SI-ActiveD(config-fw-2)# exit
SI-ActiveD(config)# vlan 1 name DEFAULT-VLAN by port
SI-ActiveD(config-vlan-1)# always-active
SI-ActiveD(config-vlan-1)# no spanning-tree
SI-ActiveD(config-vlan-1)# static-mac-address 0004.80ed.17b4 ethernet 3/1
priority 1 router-type
SI-ActiveD(config-vlan-1)# static-mac-address 0004.80f0.4b3c ethernet 3/2
priority 1 router-type
SI-ActiveD(config-vlan-1)# static-mac-address 0004.80ed.1368 ethernet 3/3
priority 1 router-type
SI-ActiveD(config-vlan-1)# static-mac-address 0004.80eb.5294 ethernet 3/4
priority 1 router-type
SI-ActiveD(config-vlan-1)# exit
SI-ActiveD(config)# vlan 999 by port
SI-ActiveD(config-vlan-999)# untagged ethe 2/5 to 2/8
SI-ActiveD(config-vlan-999)# no spanning-tree
SI-ActiveD(config-vlan-999)# exit
SI-ActiveD(config)# hostname Int-SI-D
SI-ActiveD(config)# ip address 10.10.8.222 255.255.255.0
SI-ActiveD(config)# ip default-gateway 10.10.8.120
SI-ActiveD(config)# write memory
SI-ActiveD(config)# end
SI-ActiveD(config)# reload
```

Configuring active-active HA FWLB with VRRP

This section shows examples of commonly used ServerIron ADX IronClad FWLB deployments with Layer 3 configurations. The ServerIronADXs in these examples perform Layer 3 routing in addition to Layer 2 and Layer 4–7 switching.

Generally, the steps for configuring Layer 4–7 features on a ServerIronADX running Layer 3 are similar to the steps on a ServerIronADX that is not running Layer 3. The examples focus on the Layer 3 aspects of the configurations.

NOTE
The configurations shown in these examples are the ones that are supported. If you need to use the ServerIron ADX's Layer 3 routing support in a FWLB configuration that is not shown, contact Brocade.

Overview of active-active FWLB with VRRP

Figure 12 shows an example of an active-active FWLB configuration that uses Virtual Router Redundancy Protocol (VRRP). Each pair of ServerIron ADXs provides redundant FWLB, while VRRP on the external pair of ServerIron ADXs provides redundancy for the default gateway address used by the client.

FIGURE 12   Active-active FWLB with VRRP
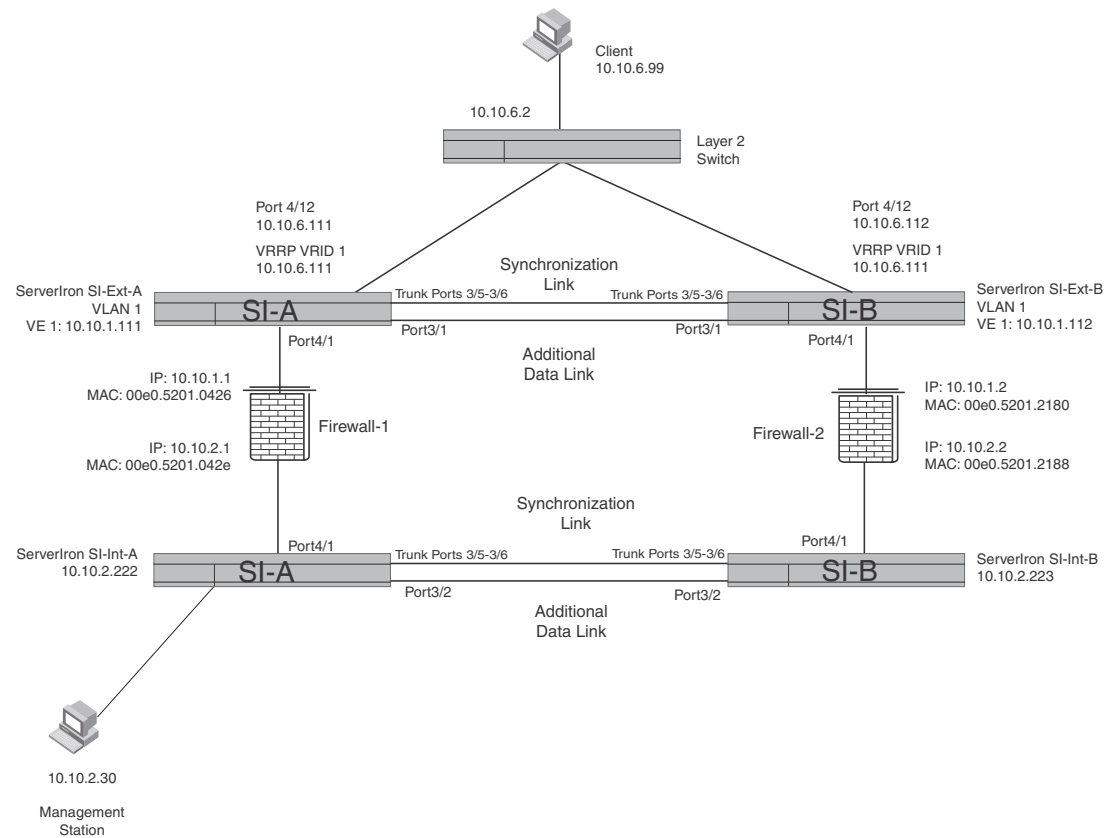
Commands on external ServerIron ADX A (SI-Ext-A)

The following commands change the CLI to the global CONFIG level, and then change the host name to "SI-Ext-A".

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-A
```

The following commands enable the always-active feature and disable the Spanning Tree Protocol (STP) in VLAN 1, which contains the ports that will carry the FWLB traffic.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# always-active
SI-Ext-A(config-vlan-1)# no spanning-tree
```

The following commands configure a virtual routing interface on VLAN 1 (the default VLAN), and then configure an IP address on the interface. The virtual routing interface is associated with all the ports in the VLAN.

```
SI-Ext-A(config-vlan-1)# router-interface ve 1
SI-Ext-A(config-vlan-1)# exit
SI-Ext-A(config)# interface ve 1
SI-Ext-A(config-ve-1)# ip address 10.10.1.111 255.255.255.0
SI-Ext-A(config-ve-1)# exit
```

The following command configures an IP default route. The next hop for this route is the ServerIron ADX's interface with firewall FW1.

```
SI-Ext-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
```

The following commands configure port-based VLAN 2, which will contain the port on which VRRP VRID 1 (10.10.6.111) is configured.

```
SI-Ext-A(config)# vlan 2
SI-Ext-A(config-vlan-2)# untag ethernet 4/12
SI-Ext-A(config-vlan-2)# exit
```

The following commands configure the dedicated synchronization link between the ServerIron ADX and its active-active partner. The **trunk** command configures the two ports of the link into a trunk group. The next two commands add the trunk group to a separate port-based VLAN, because the synchronization link must be in its own VLAN. The **server fw-port** command identifies the port number of the link. If the link is a trunk group, you must specify the MAC address of the group's primary port.

```
SI-Ext-A(config)# trunk switch ethernet 3/5 to 3/6
SI-Ext-A(config)# trunk deploy
SI-Ext-A(config)# vlan 10
SI-Ext-A(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Ext-A(config-vlan-10)# exit
SI-Ext-A(config)# server fw-port 3/5
```

The following command configures the data link between this ServerIron ADX and its active-active partner. You must use the **server partner-ports** command to specify all the data links with the partner. However, do not use the command for the synchronization link.

```
SI-Ext-A(config)# server partner-ports ethernet 3/1
```

The following commands add the firewall definitions. In this example, port HTTP is specified for each firewall. Specifying the application ports on the firewalls is optional. The **port http no-health-check** command under each firewall disables the Layer 4 health check for the HTTP port. When you add an application port to a firewall definition, the ServerIron ADX automatically enables the Layer 4 health check for that port. You must disable the Layer 4 health check if the firewall is unable to act as a proxy for the application and respond to the health check. If the firewall does not respond to the health check, the ServerIron ADX assumes that the port is unavailable and stops sending traffic for the port to the firewall.

The ServerIron ADX will still use a Layer 3 health check (IP ping) to test connectivity to the firewall.

```
SI-Ext-A(config)# server fw-name fw1 10.10.1.1
SI-Ext-A(config-rs-fw1)# port http
SI-Ext-A(config-rs-fw1)# port http no-health-check
SI-Ext-A(config-rs-fw1)# exit
SI-Ext-A(config)# server fw-name fw2 10.10.1.2
SI-Ext-A(config-rs-fw2)# port http
SI-Ext-A(config-rs-fw2)# port http no-health-check
SI-Ext-A(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group (group 2 for IPv4 addresses and group 4 for IPv6 addresses). The firewall group contains all the ports in VLAN 1 (the default VLAN).

```
SI-Ext-A(config)# server fw-group 2
SI-Ext-A(config-fw-2)# fw-name fw1
SI-Ext-A(config-fw-2)# fw-name fw2
```

The following command enables the active-active mode.

```
SI-Ext-A(config-fw-2)# sym-priority 255
```

NOTE
Do not use the same number on both ServerIron ADXs. For example, enter **sym-priority 1** on one of the ServerIron ADXs and **sym-priority 255** on the other ServerIron ADX.

The following commands add the paths through the firewalls to the other ServerIron ADX. Each path consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next-hop IP address. In this example, the topology does not contain routers other than the ServerIron ADXs. If your topology contains other routers, configure firewall paths for the routers too. For router paths, use the same IP address as the path destination and the next hop.

NOTE
The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
SI-Ext-A(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 2 3/1 10.10.2.222 10.10.1.2
SI-Ext-A(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 4 3/1 10.10.2.223 10.10.1.2
```

The following command sets the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. Because the previous firewall definitions specify the HTTP service, the ServerIron ADX will load balance requests based on the firewall that has fewer HTTP session entries in the ServerIron ADX session table.

```
SI-Ext-A(config-fw-2)# fw-predictor per-service-least-conn
```

The following command is part of the always-active feature, which provides the additional data link between this ServerIron ADX and its partner.

```
SI-Ext-A(config-fw-2)# l2-fwall
SI-Ext-A(config-fw-2)# exit
```

The following commands add static MAC entries for the firewall interfaces with the ServerIron ADX. The static MAC entries are required only if the configuration uses static routes and a single virtual routing interface, as in this example, and if the default gateway for the client or server is the firewall. If the configuration uses a dynamic routing protocol (for example, RIP or OSPF), the static entries are not required. Alternatively, the static entries are not required if you use the ServerIron ADX itself as the default gateway for the client or the server. For example, the static entries are not required if you configure the client to use 10.10.1.111 as its default gateway.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# static-mac-address 00e0.5201.0426 ethernet 4/1
priority 1 router-type
SI-Ext-A(config-vlan-1)# static-mac-address 00e0.5201.2180 ethernet 3/1
priority 1 router-type
SI-Ext-A(config-vlan-1)# exit
```

The following commands configure the VRRP parameters. The address indicated by the **ip-address** command (10.10.6.111) is the address that will be backed up by VRRP. Because this ServerIron ADX is the owner of the backed-up address, the address is configured on the port (this port owns the address) and the address is assigned to the VRID. On external ServerIron ADX B, the VRID will be configured as a backup for 10.10.6.111. The port on which the VRID is configured will have an IP address that is in the same sub-net as the backed-up address, but not the same address.

```
ServerIronADXA(config)# router vrrp
ServerIronADXA(config)# interface ethernet 4/12
ServerIronADXA(config-if-4/12)# ip address 10.10.6.111/24
ServerIronADXA(config-if-4/12)# ip vrrp vrid 1
ServerIronADXA(config-if-4/12-vrid-1)# owner
ServerIronADXA(config-if-4/12-vrid-1)# ip-address 10.10.6.111
ServerIronADXA(config-if-4/12-vrid-1)# activate
ServerIronADXA(config-if-4/12-vrid-1)# exit
ServerIronADXA(config-if-4/12)# exit
```

The following command saves the configuration changes to the startup-config file.

```
SI-Ext-A(config)# write memory
```

Commands on external ServerIron ADX B (SI-Ext-B)

The following commands configure SI-Ext-B. The SLB configuration is identical to the one on SI-Ext-A.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-B
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# always-active
SI-Ext-B(config-vlan-1)# no spanning-tree
SI-Ext-B(config-vlan-1)# router-interface ve 1
SI-Ext-B(config-vlan-1)# exit
SI-Ext-B(config)# interface ve 1
SI-Ext-B(config-ve-1)# ip address 10.10.1.112 255.255.255.0
SI-Ext-B(config-ve-1)# exit
SI-Ext-B(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
SI-Ext-B(config)# vlan 2
SI-Ext-B(config-vlan-2)# untag ethernet 4/12
SI-Ext-B(config-vlan-2)# exit
SI-Ext-B(config)# trunk switch ethernet 3/5 to 3/6
SI-Ext-B(config)# trunk deploy
SI-Ext-B(config)# vlan 10
SI-Ext-B(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Ext-B(config-vlan-10)# exit
SI-Ext-B(config)# server fw-port 3/5
SI-Ext-B(config)# server partner-ports ethernet 3/1
SI-Ext-B(config)# server fw-name fw1 10.10.1.1
SI-Ext-B(config-rs-fw1)# port http
SI-Ext-B(config-rs-fw1)# port http no-health-check
SI-Ext-B(config-rs-fw1)# exit
SI-Ext-B(config)# server fw-name fw2 10.10.1.2
SI-Ext-B(config-rs-fw2)# port http
SI-Ext-B(config-rs-fw2)# port http no-health-check
SI-Ext-B(config-rs-fw2)# exit
SI-Ext-B(config)# server fw-group 2
SI-Ext-B(config-fw-2)# fw-name fw1
SI-Ext-B(config-fw-2)# fw-name fw2
```

```
SI-Ext-B(config-fw-2)# sym-priority 1
SI-Ext-B(config-fw-2)# fwall-info 1 3/1 10.10.2.222 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 2 4/1 10.10.2.222 10.10.1.2
SI-Ext-B(config-fw-2)# fwall-info 3 3/1 10.10.2.223 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 4 4/1 10.10.2.223 10.10.1.2
SI-Ext-B(config-fw-2)# fw-predictor per-service-least-conn
SI-Ext-B(config-fw-2)# l2-fwall
SI-Ext-B(config-fw-2)# exit
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# static-mac-address 00e0.5201.0426 ethernet 3/1
priority 1 router-type
SI-Ext-B(config-vlan-1)# static-mac-address 00e0.5201.2180 ethernet 4/1
priority 1 router-type
SI-Ext-B(config-vlan-1)# exit
ServerIronADXA(config)# router vrrp
ServerIronADXA(config)# interface ethernet 4/12
ServerIronADXA(config-if-4/12)# ip address 10.10.6.112/24
ServerIronADXA(config-if-4/12)# ip vrrp vrid 1
ServerIronADXA(config-if-4/12-vrid-1)# backup
ServerIronADXA(config-if-4/12-vrid-1)# ip-address 10.10.6.111
ServerIronADXA(config-if-4/12-vrid-1)# activate
ServerIronADXA(config-if-4/12-vrid-1)# exit
ServerIronADXA(config-if-4/12)# exit
SI-Ext-B(config)# write memory
```

Usage notes

Brocade FWLB design assumes that any Network Address Translation (NAT) is performed by the load balanced firewalls, but it is not performed by the ServerIron ADXs. Under specific conditions, it is possible to use NAT pools and static entries on ServerIrons that are also engaged in FWLB.

Under the following conditions, you cannot configure the ServerIrons' VRRP or VRRP-E virtual IP address as the firewalls' default gateway:

- When the FWLB is configured
- When the VRRP or VRRP-E is configured
- When NAT is configured on the firewalls' external ServerIron ADX (for example, IP NAT is configured globally)
- When firewalls are directly connected to ServerIron ADX

If the FWLB environment meets these conditions, on the firewalls you must configure the default gateway address to be the interface address (physical or VE) of the directly connected ServerIron instead of the VRRP or VRRP-E Virtual IP. On the ServerIrons performing NAT, you must use floating default routes or some other dynamic routing protocol to maintain connectivity in case either ServerIron loses its upstream link.

Commands on internal ServerIron ADX A (SI-Int-A)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-A
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# always-active
SI-Int-A(config-vlan-1)# no spanning-tree
SI-Int-A(config-vlan-1)# router-interface ve 1
SI-Int-A(config-vlan-1)# exit
```

```
SI-Int-A(config)# interface ve 1
SI-Int-A(config-ve-1)# ip address 10.10.2.222 255.255.255.0
SI-Int-A(config-ve-1)# exit
SI-Int-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.1
SI-Int-A(config)# trunk switch ethernet 3/5 to 3/6
SI-Int-A(config)# trunk deploy
SI-Int-A(config)# vlan 10
SI-Int-A(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Int-A(config-vlan-10)# exit
SI-Int-A(config)# server fw-port 3/5
SI-Int-A(config)# server partner-ports ethernet 3/2
SI-Int-A(config)# server fw-name fw1 10.10.2.1
SI-Int-A(config-rs-fw1)# port http
SI-Int-A(config-rs-fw1)# port http no-health-check
SI-Int-A(config-rs-fw1)# exit
SI-Int-A(config)# server fw-name fw2 10.10.2.2
SI-Int-A(config-rs-fw2)# port http
SI-Int-A(config-rs-fw2)# port http no-health-check
SI-Int-A(config-rs-fw2)# exit
SI-Int-A(config)# server fw-group 2
SI-Int-A(config-fw-2)# fw-name fw1
SI-Int-A(config-fw-2)# fw-name fw2
SI-Int-A(config-fw-2)# sym-priority 255
SI-Int-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 2 3/2 10.10.1.111 10.10.2.2
SI-Int-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 4 3/2 10.10.1.112 10.10.2.2
SI-Int-A(config-fw-2)# fw-predictor per-service-least-conn
SI-Int-A(config-fw-2)# l2-fwall
SI-Int-A(config-fw-2)# exit
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# static-mac-address 00e0.5201.042e ethernet 4/1
priority 1 router-type
SI-Int-A(config-vlan-1)# static-mac-address 00e0.5201.2188 ethernet 3/2
priority 1 router-type
SI-Int-A(config-vlan-1)# exit
SI-Int-A(config)# write memory
```

Commands on internal ServerIron ADX B (SI-Int-B)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-B
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# always-active
SI-Int-B(config-vlan-1)# no spanning-tree
SI-Int-B(config-vlan-1)# router-interface ve 1
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# interface ve 1
SI-Int-B(config-ve-1)# ip address 10.10.2.223 255.255.255.0
SI-Int-B(config-ve-1)# exit
SI-Int-B(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.2
SI-Int-B(config)# trunk switch ethernet 3/5 to 3/6
SI-Int-B(config)# trunk deploy
SI-Int-B(config)# vlan 10
SI-Int-B(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Int-B(config-vlan-10)# exit
SI-Int-B(config)# server fw-port 3/5
SI-Int-B(config)# server partner-ports ethernet 3/2
```

```
SI-Int-B(config)# server fw-name fw1 10.10.2.1
SI-Int-B(config-rs-fw1)# port http
SI-Int-B(config-rs-fw1)# port http no-health-check
SI-Int-B(config-rs-fw1)# exit
SI-Int-B(config)# server fw-name fw2 10.10.2.2
SI-Int-B(config-rs-fw2)# port http
SI-Int-B(config-rs-fw2)# port http no-health-check
SI-Int-B(config-rs-fw2)# exit
SI-Int-B(config)# server fw-group 2
SI-Int-B(config-fw-2)# fw-name fw1
SI-Int-B(config-fw-2)# fw-name fw2
SI-Int-B(config-fw-2)# sym-priority 1
SI-Int-B(config-fw-2)# fwall-info 1 3/2 10.10.1.111 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 2 4/10 10.10.1.111 10.10.2.2
SI-Int-B(config-fw-2)# fwall-info 3 3/2 10.10.1.112 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 4 4/10 10.10.1.112 10.10.2.2
SI-Int-B(config-fw-2)# fw-predictor per-service-least-conn
SI-Int-B(config-fw-2)# l2-fwall
SI-Int-B(config-fw-2)# exit
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# static-mac-address 00e0.5201.042e ethernet 3/2
priority 1 router-type
SI-Int-B(config-vlan-1)# static-mac-address 00e0.5201.2188 ethernet 4/1
priority 1 router-type
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# write memory
```

Usage notes

When configuring FWLB+VRRPE+NAT, it is necessary to configure the firewalls to use interface IP addresses as default gateways:

- On the firewalls, configure the default gateway address to be the interface address (physical or VE) of the directly connected ServerIron, instead of the VRRP or VRRP-E Virtual IP.

- Assuming that the ServerIron ADXs on the outside of the firewalls are performing NAT, on each of those two ServerIrons, add an additional higher-cost default route pointing to the inside interface IP address of the partner ServerIron.

For example, assume that SI1 and SI2 are the ServerIron ADXs external to the firewalls, and their default gateway is 202.221.202.100, SI1's internal address is 10.10.1.1, and SI2's internal address is 10.10.1.2.

The following commands configure the firewalls to use interface IP addresses as default gateways on SI1:

```
ip route 0.0.0.0 0.0.0.0 202.221.202.100
ip route 0.0.0.0 0.0.0.0 10.10.1.2 10
```

The following commands configure the firewalls to use interface IP addresses as default gateways on SI2:

```
ip route 0.0.0.0 0.0.0.0 202.221.202.100
ip route 0.0.0.0 0.0.0.0 10.10.1.1 10
```

Configuring Multizone FWLB

In this chapter

Zone configuration

Multizone FWLB allows you to configure ServerIron ADXs to forward packets based on the destination zone. For example, if your network consists of an Internet side, an internal side, and a Demilitarized Zone (DMZ) in between, you can configure ServerIron ADXs to forward packets through the firewalls to the correct zone.

When you configure multizone FWLB, you first identify a zone by configuring standard Access Control Lists (ACLs). An ACL specifies the IP addresses (or address ranges) within the zone. When you configure the firewall group parameters, you add the zones and define them by associating the ACLs with them. Each zone consists of a zone number, an optional name, and a standard ACL that specifies the IP addresses contained in the zone.

You can configure multizone FWLB for basic configurations and IronClad (high-availability) configurations. This section provides an example for each type of configuration.

When the ServerIron ADX forwards a packet, it selects a path that goes through a firewall to a ServerIron ADX that is in the zone that contains the destination IP address of the packet.

The configuration tasks for multizone FWLB are the same as other FWLB implementations, with the exception of the configuration for the zones.

Consider the following when you configure zones:

- Do not define zone 1. When zone 1 is undefined, the zone by default contains all IP addresses that are not explicitly configured as members of other zones (zones 2 through 10). In typical configurations, the ServerIron ADXs in the DMZ and the internal network contain zone definitions for each other, while none of the ServerIron ADXs contains a zone definition for zone 1 (thus leaving zone 1 undefined). As a result, traffic that is not destined for an address in the DMZ or the internal network is sent to the Internet.

  You can define zone 1, but if you do, this zone contains only the IP address ranges you configure for the zone.

- Do not configure zone information on a ServerIron ADX for the zone the ServerIron ADX is in.

- On the DMZ ServerIron ADXs, configure zone definitions for the zones in the internal network and other DMZs, if applicable.

- On the internal ServerIron ADXs, configure zone definitions for the zones in the DMZs, and other internal networks, if applicable.

Generally, each ServerIron ADX should contain definitions for two less zones than the total number of zones in the network. The two zones you leave out are zone 1 (which remains undefined) and the zone the ServerIron ADX itself is in. If you are configuring a ServerIron ADX in zone 1, leave out configuration information for zone 1 and one of the other zones.

Configuring basic multizone FWLB

Figure 13 shows an example of a basic multizone FWLB configuration. In this example, each ServerIron ADX is in a separate zone:

- ServerIron ADX Zone1-SI is in zone 1. By default, zone 1 contains all IP addresses that are not members of other, user-configured zones. You can explicitly configure zone 1 but it is not necessary. In the CLI configuration example for this configuration, zone 1 is not configured. ServerIron ADX Zone1-SI contains zone definitions for zone 2 (the DMZ zone) but not for zone 1 or zone 3.

- ServerIron ADX Zone2-SI is in zone 2 (the "DMZ" zone in this example). Zone 2 contains IP addresses in the range 209.157.25.0/24 through 209.157.25.255/24. This ServerIron ADX contains configuration information for zone 3 (the internal network zone) but does not contain definitions for zone 1 (the external network zone) or zone 2 (the DMZ zone itself).

- ServerIron ADX Zone3-SI is in zone 3 (the "internal network" zone in the example). Zone 3 contains IP addresses in the range 209.157.23.0/24 through 209.157.23.255/24. This ServerIron ADX contains configuration information for zone 2 (the DMZ zone) but does not contain definitions for zone 1 (the external network zone) or zone 3 (the internal network zone itself).

When one of the ServerIron ADXs receives traffic with the destination IP address in another zone, the ServerIron ADX selects a path for the traffic based on the zone the destination IP address is in. For example, if a client on the Internet sends traffic addressed to a server in zone 2, ServerIron ADX Zone1-SI selects a path that sends the traffic through a firewall to ServerIron ADX Zone2-SI, which forwards the traffic to the server. (ServerIron ADX Zone2-SI can be configured to load balance traffic across multiple servers or can simply be used as a Layer 2 switch to forward the traffic to the server.)

When ServerIron ADX Zone2-SI forwards the server's reply to the client, the ServerIron ADX selects a path to ServerIron ADX Zone1-SI. ServerIron ADX Zone2-SI knows the traffic goes to zone 1 because the destination IP address of the traffic is not in its own sub-net (zone 2) or in zone 3.

FIGURE 13   Basic multizone FWLB configuration
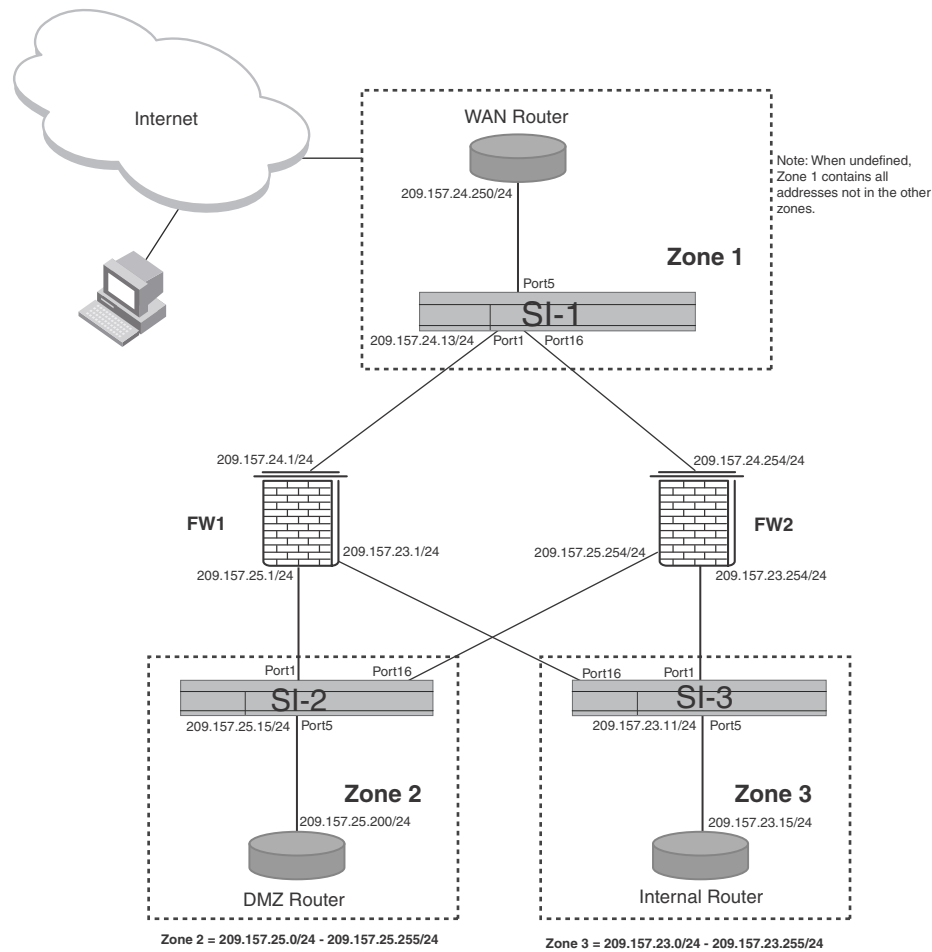
To configure ServerIron ADXs for basic multizone FWLB, perform the following tasks:

- **Configure global system parameters.**

  These parameters include the ServerIron ADX IP address and default gateway. You also need to globally disable the Spanning Tree Protocol (STP). Disabling STP is required for this configuration.

- **Configure global FWLB parameters:**
  - Globally enable FWLB.
  - Identify the port connected to the router.

- **Configure firewall parameters:**

  Define the firewalls and add them to the firewall group. Each firewall consists of a name and the IP address of its interface with the ServerIron ADX.

- **Configure a standard ACL for each zone that the ServerIron ADX is not a member, except zone 1.**

  The ACLs identify the IP addresses or address ranges in the other zones. If you leave zone 1 undefined, all IP addresses that are not in this ServerIron ADX's own sub-net and are not members of zones configured on the ServerIron ADX are assumed to be members of zone 1.

  If the ServerIron ADX is a member of zone 1, configure a standard ACL for all but one of the other zones. In this example, configure an ACL for the DMZ zone (zone 2). The ServerIron ADX will forward traffic that is not addressed to its own sub-net (zone 1), and not addressed to zone 2, to the other zone (zone 3) automatically.

- **Configure firewall group parameters:**
  - Configure the zones. Each zone definition consists of a number, an optional name, and the ACL that specifies the IP addresses in the zone. See Table 3 for the maximum number of zones and paths supported on the ServerIron ADX ADX.
  - Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX. Configure a separate path through each firewall to each ServerIron ADX. You also must configure a path from each ServerIron ADX to the routers attached to the ServerIron ADX.

- **Save the configuration to the startup-config file.**

Configuration example for basic multizone FWLB

The following sections show all the ServerIron ADX commands you would enter on each ServerIron ADX to implement the configuration shown in Figure 13 on page 73.

Most of the configuration tasks for multizone FWLB are the same as the tasks for other FWLB configurations.

Commands on ServerIron ADX Zone1-SI

The following commands configure ServerIron ADX "Zone1-SI" in zone 1 in Figure 13 on page 73.

The first set of commands changes the device name, configures the management IP address, and specifies the default gateway. Notice that the management IP address is in the same sub-net as the firewall interface with the ServerIron ADX. If the ServerIron ADX and the firewall are in different sub-nets, you need to configure source IP addresses and enable source NAT.

In this configuration, the default gateway is the IP address of one of the firewall interfaces with the ServerIron ADX. In this case, the IP address is the address of firewall FW1's interface with this ServerIron ADX.

```
ServerIronADX(config)# hostname Zone1-SI
Zone1-SI(config)# ip address 209.157.24.13 255.255.255.0
Zone1-SI(config)# ip default-gateway 209.157.24.1
```

The following command disables the Spanning Tree Protocol (STP). You must disable STP on all the devices in this type of FWLB configuration.

```
Zone1-SI(config)# no span
```

The following command identifies the router port, which is the ServerIron ADX port connected to a router. In the example in Figure 13 on page 73, each ServerIron ADX has one router port. If the link is a trunk group, enter the primary port number. In this example, the router port is port 5.

```
Zone1-SI(config)# server router-ports 5
```

The following commands add the firewalls.

```
Zone1-SI(config)# server fw-name FW1 209.157.24.1
Zone1-SI(config-rs-FW1)# exit
Zone1-SI(config)# server fw-name FW2 209.157.24.254
Zone1-SI(config-rs-FW2)# exit
```

The names are specific to the ServerIron ADX and do not need to correspond to any name parameters on the firewalls themselves. The IP addresses are the addresses of the firewall interfaces with the ServerIron ADX.

The following command configures an Access Control List (ACL) for the IP addresses in the DMZ zone (zone 2).   The command configures a standard ACL for the addresses in zone 2, which contains addresses in the 209.157.25.x/24 sub-net. The "0.0.0.255" values indicate the significant bits in the IP address you specify. In this case, all bits except the ones in the last node of the address are significant.

In this configuration, only one zone definition is required on each ServerIron ADX, including Zone1-SI. Because the Zone1-SI ServerIron ADX is already in zone 1, the ServerIron ADX will forward packets either to the ServerIron ADX in zone 2 or to the only other ServerIron ADX that is not in zone 2. In this case, the only other ServerIron ADX is the one in zone 3. Thus, if ServerIron ADX Zone1-SI receives a packet that is not addressed to the sub-net Zone1-SI is in, and is not addressed to a sub-net in zone 2, the ServerIron ADX assumes that the packet is for an address in the other zone, zone 3. The ServerIron ADX forwards the packet to the ServerIron ADX in zone 3.

```
Zone1-SI(config)# access-list 2 permit 209.157.25.0 0.0.0.255
```

Although each zone in this example contains one Class C sub-net, you can configure ACLs for any range of addresses and even for individual host addresses.

NOTE
This example shows a numbered ACL instead of a named ACL. You must use numbered ACLs. The FWLB software does not support zone configuration based on named ACLs.

The following commands configure the firewall group parameters. In this case, the commands configure the firewall zones, add zone 2, and add the firewalls.

```
Zone1-SI(config)# server fw-group 2
Zone1-SI(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI(config-fw-2)# fw-name FW1
Zone1-SI(config-fw-2)# fw-name FW2
```

Syntax: [no] fwall-zone <zone-name> <zone-number> <acl-number>

The fwall-zone command configures a firewall zone. To configure a zone, specify the following variables:

The <zone-name> variable specifies an ASCII string that identifies the zone.

The <zone-number> variable specifies the number of the zone being configured. This variable can be specified as an integer from 1 through 10. Refer to Table 3 for the maximum number of zones and paths supported on the ServerIron ADX ADX.

The <acl-number> variable specifies the standard ACL that specifies the IP addresses in the zone.

In this example, the ACL number and zone number are the same, but this is not required.

Syntax: [no] fw-name *<firewall-name>*

The **fw-name** command adds the previously configured firewalls to the firewall group.

Specify the names you entered when configuring the firewalls for the *<firewall-name>* variable. In this example, the names are "FW1" and "FW2".

The following commands configure the firewall paths. In the configuration in , each ServerIron ADX has five paths:

- A path through FW1 to ServerIron ADX Zone2
- A path through FW2 to ServerIron ADX Zone2
- A path through FW1 to ServerIron ADX Zone3
- A path through FW2 to ServerIron ADX Zone3
- A path to the router

The ServerIron ADX uses the firewall paths to load balance the firewall traffic across the two firewalls. As in other types of FWLB configurations, the paths must be fully meshed among the ServerIron ADXs and firewalls. Thus, the ServerIron ADX has a separate path through each of the firewalls to each of the ServerIron ADXs in the other zones.

The ServerIron ADX also uses the paths for checking the health of the links. The health checking enables the ServerIron ADX to compensate if the link to a firewall becomes unavailable by sending traffic that normally goes through the unavailable firewall through the firewall that is still available.

```
Zone1-SI(config-fw-2)# fwall-info 1 1 209.157.25.15 209.157.24.1
Zone1-SI(config-fw-2)# fwall-info 2 1 209.157.23.11 209.157.24.1
Zone1-SI(config-fw-2)# fwall-info 3 16 209.157.25.15 209.157.24.254
Zone1-SI(config-fw-2)# fwall-info 4 16 209.157.23.11 209.157.24.254
Zone1-SI(config-fw-2)# fwall-info 5 5 209.157.24.250 209.157.24.250
Zone1-SI(config-fw-2)# exit
```

Each **fwall-info** command consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next hop IP address. The paths that pass through FW1 use ServerIron ADX port 1, which is connected to FW1. The paths that pass through FW2 use ServerIron ADX port 16.

Notice that the last path, unlike the other paths, has the same IP address for the destination and the next-hop for the path. This path is a router path and ends at the router itself. The other paths are firewall paths and end at the ServerIron ADX at the other end of the firewall.

The following commands add static entries to the ServerIron ADX's MAC table for the firewall interfaces.

```
Zone1-SI(config)# static-mac-address abcd.5200.348d ethernet 1 priority 1
router-type
Zone1-SI(config)# static-mac-address abcd.5200.0b50 ethernet 16 priority 1
router-type
```

Each command includes the MAC address of the firewall's interface with the ServerIron ADX and the ServerIron ADX port that is connected to the firewall. The **priority 1** and **router-type** parameters identify the MAC entry type and are required.

The following command saves the configuration information to the ServerIron ADX's startup-config file on flash memory. You must save the configuration information before reloading the software or powering down the device. Otherwise, the information is lost.

```
Zone1-SI(config)# write memory
```

Commands on Zone2-SI in zone 2

The following commands configure ServerIron ADX "Zone2-SI" in zone 2 in Figure 13 on page 73. The configuration is similar to the one for Zone1-SI, with the following exceptions:

- The management IP address is different.

- The default gateway goes to a different interface on FW1.

- The paths are different due to the ServerIron ADX's placement in the network. (However, like Zone1-SI, ServerIron ADX Zone2-SI has a path through each firewall to the ServerIron ADXs in the other zones, and has a path to its directly attached router.)

- An ACL and zone definition are configured for zone 3. Because this ServerIron ADX is in zone 2, the configuration does not include an ACL and zone definition for zone 2. This ServerIron ADX also does not contain an ACL or zone definition for zone 1. As a result, by default, this ServerIron ADX forwards packets that are not addressed to the ServerIron ADX's own sub-net, or to a sub-net in zone 3, to zone 1.

```
ServerIronADX(config)# hostname Zone2-SI
Zone2-SI(config)# ip address 209.157.24.15 255.255.255.0
Zone2-SI(config)# ip default-gateway 209.157.25.1
Zone2-SI(config)# no span
Zone2-SI(config)# server router-ports 5
Zone2-SI(config)# server fw-name FW1 209.157.25.1
Zone2-SI(config-rs-FW1)# exit
Zone2-SI(config)# server fw-name FW2 209.157.25.254
Zone2-SI(config-rs-FW2)# exit
Zone2-SI(config)# access-list 3 permit 209.157.23.0 0.0.0.255
Zone2-SI(config)# server fw-group 2
Zone2-SI(config-fw-2)# fwall-zone Zone3 3 3
Zone2-SI(config-fw-2)# fw-name FW1
Zone2-SI(config-fw-2)# fw-name FW2
Zone2-SI(config-fw-2)# fwall-info 1 1 209.157.25.15 209.157.24.1
Zone2-SI(config-fw-2)# fwall-info 2 16 209.157.23.11 209.157.24.1
Zone2-SI(config-fw-2)# fwall-info 3 16 209.157.25.15 209.157.24.254
Zone2-SI(config-fw-2)# fwall-info 4 1 209.157.23.11 209.157.24.254
Zone2-SI(config-fw-2)# fwall-info 5 5 209.157.25.200 209.157.25.200
Zone2-SI(config-fw-2)# exit
Zone2-SI(config)# static-mac-address abcd.5200.348b ethernet 1 priority 1
router-type
Zone2-SI(config)# static-mac-address abcd.5200.0b4e ethernet 16 priority 1
router-type
Zone2-SI(config)# write memory
Zone2-SI(config)# exit
```

Commands on Zone3-SI in zone 3

The following commands configure ServerIron ADX "Zone3-SI" in zone 3 in Figure 13 on page 73. The configuration is similar to the ones for the other ServerIron ADXs, with the following exceptions:

- The management IP address is different.

- The default gateway goes to an interface on FW2.

- The paths are different due to the ServerIron ADX's placement in the network.

- An ACL and zone definition are configured for zone 2. Because this ServerIron ADX is in zone 3, the configuration does not include an ACL and zone definition for the zone. This ServerIron ADX also does not contain an ACL or zone definition for zone 1. As a result, by default, this ServerIron ADX forwards packets that are not addressed to the ServerIron ADX's own sub-net, or to a sub-net in zone 2, to zone 1.

```
ServerIronADX(config)# hostname Zone3-SI
Zone3-SI(config)# ip address 209.157.23.11 255.255.255.0
Zone3-SI(config)# ip default-gateway 209.157.23.1
Zone3-SI(config)# no span
Zone3-SI(config)# server router-ports 5
Zone3-SI(config)# server fw-name FW1 209.157.23.1
Zone3-SI(config-rs-FW1)# exit
Zone3-SI(config)# server fw-name FW2 209.157.23.254
Zone3-SI(config-rs-FW2)# exit
Zone3-SI(config)# access-list 2 permit 209.157.25.0 0.0.0.255
Zone3-SI(config)# server fw-group 2
Zone3-SI(config-fw-2)# fwall-zone Zone2 2 2
Zone3-SI(config-fw-2)# fw-name FW1
Zone3-SI(config-fw-2)# fw-name FW2
Zone3-SI(config-fw-2)# fwall-info 1 16 209.157.24.13 209.157.23.1
Zone3-SI(config-fw-2)# fwall-info 2 1 209.157.24.13 209.157.23.254
Zone3-SI(config-fw-2)# fwall-info 3 16 209.157.25.15 209.157.23.1
Zone3-SI(config-fw-2)# fwall-info 4 1 209.157.25.15 209.157.23.254
Zone3-SI(config-fw-2)# fwall-info 5 5 209.157.23.15 209.157.23.15
Zone3-SI(config-fw-2)# exit
Zone3-SI(config)# static-mac-address abcd.5200.3489 ethernet 16 priority 1
router-type
Zone3-SI(config)# static-mac-address abcd.5200.0b4c ethernet 1 priority 1
router-type
Zone3-SI(config)# write memory
Zone3-SI(config)# exit
```

Configuring highly-availability multizone FWLB

Figure 14 on page 79 shows an example of a high-availability multizone FWLB configuration. This example has the same zones as the basic example in Figure 13 on page 73, but in the high-availability configuration, each zone contains a pair of active-standby ServerIron ADXs instead of a single ServerIron ADX.

In this configuration, the ServerIron ADXs on the left side of Figure 14 are the active ServerIron ADXs. The ServerIron ADXs on the right are the standby ServerIron ADXs. Each active-standby pair is connected by a private link, which the ServerIron ADXs use to exchange failover information. The ports used by the private links are in their own port-based VLAN, separate from the other ServerIron ADX ports. Add the ports as untagged ports. For added redundancy, the private links also are configured as two-port trunk groups.

This example also uses a simplified topology. Instead of using Layer 2 switches and redundant links to provide failover data paths from the devices on the left side to the devices on the right side, this configuration uses additional links between the ServerIron ADXs. The **l2-fwall** and **always-active** commands enable you to use this type of simplified topology. The *l2-fwall* command prevents data loops by blocking traffic on the standby ServerIron ADX, while the *always-active* command allows the standby ServerIron ADXs to pass traffic to their active partners for forwarding.

FIGURE 14   **High-availability configuration with separate firewall zones**
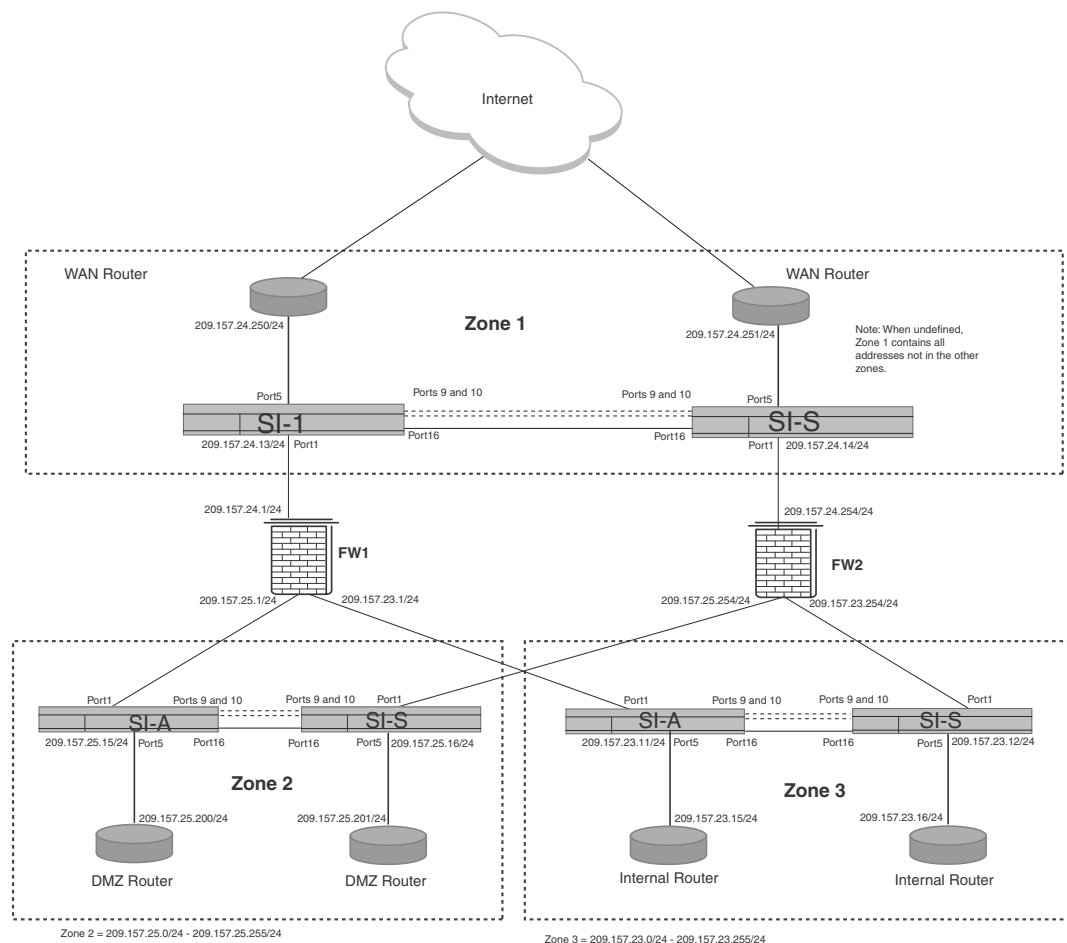
To configure ServerIron ADXs for IronClad multizone FWLB, perform the following tasks:

- Configure global system parameters.

  These parameters include the ServerIron ADX IP address and default gateway. You also need to globally disable the Spanning Tree Protocol (STP). Disabling STP is required for this configuration.

- Configure global FWLB parameters:

  - Identify the synchronization port, which is the port connected to this ServerIron ADX's high-availability partner and place the port in a separate Layer port-based VLAN, as an untagged port. (This task applies only to high-availability configurations.)

  - Identify the port connected to the router.

  - Enable the always-active feature for the VLAN that contains all the ports except the synchronization link.

- Configure a standard ACL for each zone that the ServerIron ADX is not a member, except zone 1.

  The ACLs identify the IP addresses or address ranges in the other zones. If you leave zone 1 undefined, all IP addresses that are not in this ServerIron ADX's own sub-net and are not members of zones configured on the ServerIron ADX are assumed to be members of zone 1.

  If the ServerIron ADX is a member of zone 1, configure a standard ACL for all but one of the other zones. In this example, configure an ACL for the DMZ zone (zone 3). The ServerIron ADX will forward traffic that is not addressed to its own sub-net, and not addressed to zone 2, to the other zone (zone 3) automatically.

- Configure firewall parameters:

  Define the firewalls and add them to the firewall group. Each firewall consists of a name and the IP address of its interface with the ServerIron ADX.

- Configure firewall group parameters:

  - Configure the zones. Each zone definition consists of a number, an optional name, and the ACL that specifies the IP addresses in the zone. Refer to Table 3 for the maximum number of zones and paths supported on the ServerIron ADX ADX.

  - Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX. Configure a separate path through each firewall to each ServerIron ADX. You also need to configure a path from each ServerIron ADX to the routers attached to the ServerIron ADX.

  - Specify the ServerIron ADX priority. The ServerIron ADX with the higher priority value is the ServerIron ADX in the active-standby pair that is active by default.

- Save the configuration to the startup-config file.

Failover algorithm

ServerIron ADXs in high-availability multizone FWLB configurations use the following criteria for failover:

- Connection to zones – If one ServerIron ADX in an active-standby ServerIron ADX has connectivity to more zones than the other ServerIron ADX, the ServerIron ADX with connectivity to more zones is the active ServerIron ADX.

- Total number of good paths – If each ServerIron ADX has connectivity to an equal number of zones, the ServerIron ADX with more good paths, within the configured tolerance, is the active ServerIron ADX. The paths include firewall paths and router paths. By default, the ServerIron ADXs can tolerate up to half of the firewall paths and half the router paths being down before failover based on good paths occurs. You can change the path tolerance.

- Priority – If all the previous metrics are equal on each ServerIron ADX, the ServerIron ADX with the higher priority is the active ServerIron ADX.

Configuration example for a high-availability multizone FWLB

The following sections show all the ServerIron ADX commands you would enter on each ServerIron ADX to implement the configuration shown in Figure 14 on page 79.

Most of the configuration tasks for high-availability multizone FWLB are the same as the tasks for other FWLB configurations.

Commands on Zone1-SI-A zone 1

The following commands configure ServerIron ADX "Zone1-SI-A" on the left side of zone 1 in Figure 14 on page 79.

The following commands change the device name, configure the management IP address, and specify the default gateway. Notice that the management IP address is in the same sub-net as the firewall interface with the ServerIron ADX. If the ServerIron ADX and the firewall are in different sub-nets, you must configure source IP addresses and enable source NAT.

In this configuration, the default gateway for each ServerIron ADX is the IP address of the firewall interface with that ServerIron ADX. In this case, the IP address is the address of firewall FW1's interface with this ServerIron ADX.

```
ServerIronADX(config)# hostname Zone1-SI-A
Zone1-SI-A(config)# ip address 209.157.24.13 255.255.255.0
Zone1-SI-A(config)# ip default-gateway 209.157.24.1
```

The following command disables the Spanning Tree Protocol (STP). You must disable STP on all the devices in this type of FWLB configuration.

```
Zone1-SI-A(config)# no span
```

The following command identifies the router port, which is the ServerIron ADX port connected to a router. In the example in Figure 14 on page 79, each ServerIron ADX has one router port.

```
Zone1-SI-A(config)# server router-ports 5
```

The following commands identify the port for the link to the other ServerIron ADX. If the link is a trunk group, enter the primary port number. In this example, the link is a trunk group made of ports 9 and 10, but you only need to specify port 9, the trunk group's primary port.

The commands also create a trunk group for the ports that connect this ServerIron ADX to its high-availability partner, then create a separate port-based VLAN containing the ports in the trunk group. Always configure the private link between the active and standby ServerIron ADX in a separate port-based VLAN. Add the ports as untagged ports.

Using a trunk group for the link between the active and standby ServerIron ADXs is not required, but using a trunk group adds an additional level of redundancy for enhanced availability. If one of the ports in a trunk group goes down, the link remains intact as long as the other port remains up. Make sure you configure a server trunk group, not a switch trunk group. The default trunk group type is switch, so you must specify the **server** option.

Notice that the **server fw-port** command (which identifies the port connected to the other ServerIron ADX) refers to only one port, even though the link is actually a multiple-port trunk group. This port number is the primary port of the trunk group. If you use a trunk group for the private link between the active and standby ServerIron ADXs, refer to the group by its primary port; in this case, port 9.

```
Zone1-SI-A(config)# server fw-port 9
Zone1-SI-A(config)# trunk server ethernet 9 to 10
Zone1-SI-A(config)# trunk deploy
Zone1-SI-A(config)# vlan 10 by port
Zone1-SI-A(config-vlan-10)# untagged 9 to 10
Zone1-SI-A(config-vlan-10)# exit
```

The following commands enable the always-active option on the default VLAN.

The default VLAN contains all the ports you have not placed in other port-based VLANs. In this configuration, the default VLAN contains all ports except ports 9 and 10, which are used for the private link between the active and standby ServerIron ADXs.

The **always-active** command enables the standby ServerIron ADX to forward traffic by sending it through the active ServerIron ADX. This command is useful in configurations where you need to enable the **l2-fwall** command (to prevent Layer 2 loops through the standby ServerIron ADX), but you also must allow traffic to pass through the standby ServerIron ADX because that ServerIron ADX is the only path for some traffic.

Without the **always-active** command, the standby ServerIron ADX blocks all traffic. As a result, if the router connected to the standby ServerIron ADX forwards client traffic addressed to a server in the DMZ, the traffic is blocked by the standby ServerIron ADX. However, when the **always-active** command is enabled, the standby ServerIron ADX forwards traffic to its active partner ServerIron ADX, which then forwards the traffic to its destination.

In some configurations, you do not need the **l2-fwall** command or the always-active command. However, configurations that do not use these commands compensate with redundant links and sometimes extra Layer 2 switches. For example, if each ServerIron ADX in Figure 14 on page 79 had links to both routers in its zone and also to both firewalls, and if Layer 2 switches were added to the configuration to allow STP to prevent Layer 2 loops, then it is possible that neither the **l2-fwall** command nor the **always-active** command would be required.

In the configuration in Figure 14 on page 79, each router and firewall is connected to only one of the two ServerIron ADXs in an active-standby pair. Neither the routers nor the firewalls have direct links (or links through Layer 2 switches) to both the active and standby ServerIron ADXs in their zones.

Using the **l2-fwall** and **always-active** commands allows you to simplify the network topology while still obtaining the benefits of the IronClad (high-availability) configuration.   Use the following commands to enable the always-active option in the default VLAN (VLAN 1). You enable the L2-fwall option when you configure firewall group parameters (see the following example).

```
Zone1-SI-A(config)# vlan 1
Zone1-SI-A(config-vlan-1)# always-active
Zone1-SI-A(config-vlan-1)# exit
```

The following commands add the firewalls.

```
Zone1-SI-A(config)# server fw-name FW1 209.157.24.1
Zone1-SI-A(config-rs-FW1)# exit
Zone1-SI-A(config)# server fw-name FW2 209.157.24.254
Zone1-SI-A(config-rs-FW2)# exit
```

The names are specific to the ServerIron ADX and do not need to correspond to any name parameters on the firewalls themselves. The IP addresses are the addresses of the firewall interfaces with the ServerIron ADX.

The following command configures an Access Control List (ACL) for the IP addresses in one of the zones this ServerIron ADX is not in. In this configuration, only one zone definition is required on each ServerIron ADX, including Zone1-SI-A and Zone1-SI-S. Because the active Zone 1 ServerIron ADX is already in zone 1, the ServerIron ADX will forward packets either to the active ServerIron ADX in zone 2 or to the only other active ServerIron ADX that is not in zone 2. In this case, that other active ServerIron ADX is in zone 3. Thus, if ServerIron ADX Zone1-SI-A receives a packet that is not addressed to the sub-net Zone1-SI-A is in, and is not addressed to a sub-net in zone 2, the ServerIron ADX assumes that the packet is for an address in the other zone, zone 3. The ServerIron ADX forwards the packet to the ServerIron ADX in zone 3.

The command configures an ACL for the addresses in zone 2, which contains addresses in the 209.157.25.x/24 sub-net. The "0.0.0.255" values indicate the significant bits in the IP address you specify. In this case, all bits except the ones in the last node of the address are significant.

```
Zone1-SI-A(config)# access-list 2 permit 209.157.25.0 0.0.0.255
```

Although each zone in this example contains one Class C sub-net, you can configure ACLs for any range of addresses and even for individual host addresses.

NOTE
This example shows a numbered ACL instead of a named ACL. You must use numbered ACLs. The FWLB software does not support zone configuration based on named ACLs.

The following commands configure the firewall group parameters. In this case, the commands configure the firewall zones, add the firewalls, enable the L2-fwall option, and set the active-standby priority.

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-A(config-fw-2)# fw-name FW1
Zone1-SI-A(config-fw-2)# fw-name FW2
Zone1-SI-A(config-fw-2)# l2-fwall
Zone1-SI-A(config-fw-2)# sym-priority 255
```

The **fwall-zone** command configures a firewall zone. To configure a zone, specify a name for the zone, and then a zone number (from 1 through 10), followed by the number of the standard ACL that specifies the IP addresses in the zone. In this example, the ACL numbers and zone numbers are the same, but this is not required.

The **fw-name** commands add the firewalls. Specify the names you entered when configuring the firewalls. In this example, the names are "FW1" and "FW2".

The **l2-fwall** command enables the L2-fwall option. This option blocks the Layer 2 traffic on the standby ServerIron ADXs. If you do not enable this mode, Layer 2 traffic can pass through the ServerIron ADXs, causing loops. Layer 3 traffic is automatically blocked on the standby ServerIron ADXs, so you do not need to explicitly block the traffic. The always-active option (enabled in the default VLAN in commands described previously) allows the standby ServerIron ADX to still forward traffic by sending the traffic to the active ServerIron ADX over the private link between the ServerIron ADXs.

The **sym-priority** command enables the active-active mode. The priority can be from 0 through 255. For details about configuring this command, refer to "Enabling the active-active mode" on page 48

NOTE
If you specify 0, the CLI removes the priority. When you save the configuration to the startup-config file, the **sym-priority** command is removed. You cannot remove the priority using the **no sym-priority** command.

The following commands configure the firewall paths. In the configuration in Figure 14 on page 79, each ServerIron ADX has nine paths:

- A path through FW1 to ServerIron ADX Zone3-SI-A, the active ServerIron ADX in zone 3
- A path through FW2 to ServerIron ADX Zone3-SI-A (This path passes through the standby ServerIron ADX, then through FW2.)
- A path through FW1 to ServerIron ADX Zone3-SI-S, the standby ServerIron ADX in zone 3
- A path through FW2 to ServerIron ADX Zone3-SI-S (This path passes through the standby ServerIron ADX.)
- A path through FW1 to ServerIron ADX Zone2-SI-A.
- A path through FW2 to ServerIron ADX Zone2-SI-A
- A path through FW1 to ServerIron ADX Zone2-SI-S
- A path through FW2 to ServerIron ADX Zone2-SI-S
- A path to the router

The ServerIron ADX uses the firewall paths to load balance the firewall traffic across the two firewalls. As in other types of FWLB configurations, the paths must be fully meshed among the ServerIron ADXs and firewalls. Thus, the ServerIron ADX has a separate path through each of the firewalls to each of the ServerIron ADXs in the other zones.

The ServerIron ADX also uses the paths for checking the health of the links. The health checking enables the ServerIron ADX to compensate if the link to a firewall becomes unavailable by sending traffic that normally goes through the unavailable firewall through the firewall that is still available. The results of the path health checks also play a role in the failover mechanism. The ServerIron ADX determines how many zones it can access and how many firewall and router paths are good based on health checks of the paths. If a path fails a health check, this can result in a failover to the other ServerIron ADX. (Refer to "Failover algorithm" on page 81.)

```
Zone1-SI-A(config-fw-2)# fwall-info 1 1 209.157.23.11 209.157.24.1
Zone1-SI-A(config-fw-2)# fwall-info 2 1 209.157.23.12 209.157.24.1
Zone1-SI-A(config-fw-2)# fwall-info 3 16 209.157.23.11 209.157.24.254
Zone1-SI-A(config-fw-2)# fwall-info 4 16 209.157.23.12 209.157.24.254
Zone1-SI-A(config-fw-2)# fwall-info 5 1 209.157.25.15 209.157.24.1
Zone1-SI-A(config-fw-2)# fwall-info 6 1 209.157.25.16 209.157.24.1
```

```
Zone1-SI-A(config-fw-2)# fwall-info 7 16 209.157.25.15 209.157.24.254
Zone1-SI-A(config-fw-2)# fwall-info 8 16 209.157.25.16 209.157.24.254
Zone1-SI-A(config-fw-2)# fwall-info 9 5 209.157.24.250 209.157.24.250
Zone1-SI-A(config-fw-2)# exit
```

Each **fwall-info** command consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next-hop IP address. The paths that pass through FW1 use ServerIron ADX port 1, which is connected to FW1. The paths that pass through FW2 (by way of the standby ServerIron ADX, Zone1-SI-S) use ServerIron ADX port 16, which is connected to Zone1-SI-S. Note that the connection on port 16 is different from the private link between the two ServerIron ADXs on ports 9 and 10. The connection on port 16 is in the same VLAN as the links to the routers and firewalls (the default VLAN, VLAN 1). The private link on ports 9 and 10 is in a separate port-based VLAN and is not used in any of the paths. The private link on ports 9 and 10 in VLAN 2 is used only to exchange failover information. All traffic between zones uses the links in the default VLAN.

Notice that the last path, unlike the other paths, has the same IP address for the destination and the next hop for the path. This path is a router path and ends at the router itself. The other paths are firewall paths and end at the ServerIron ADX at the other end of the firewall.

The following commands add static entries to the ServerIron ADX's MAC table for the firewall interfaces.

```
Zone1-SI-A(config)# vlan 1
Zone1-SI-A(config-vlan-1)# static-mac-address abcd.5200.348d ethernet 1 priority
1 router-type
Zone1-SI-A(config-vlan-1)# static-mac-address abcd.5200.0b50 ethernet 16 priority
1 router-type
Zone1-SI-A(config-vlan-1)# exit
```

Each command includes the MAC address of the firewall's interface with the ServerIron ADX and the ServerIron ADX port that is connected to the firewall. The **priority 1** and **router-type** parameters identify the MAC entry type and are required.

NOTE
If you enter the **static-mac-address** command at the global CONFIG level, the static MAC entry applies to the default port-based VLAN (VLAN 1). If you enter the **static-mac-address** command at the configuration level for a specific port-based VLAN, the entry applies to that VLAN and not to the default VLAN.

The following command saves the configuration information to the ServerIron ADX's startup-config file on flash memory. You must save the configuration information before reloading the software or powering down the device. Otherwise, the information is lost.

```
Zone1-SI-A(config)# write memory
```

The following commands change the CLI to the Privileged EXEC level, and reload the software. Because this configuration includes a trunk group, you must reload the software to place the trunk group into effect.

```
Zone1-SI-A(config)# exit
Zone1-SI-A# reload
```

Commands on Zone1-SI-S in zone 1

The following commands configure ServerIron ADX "Zone1-SI-S" on the right side of zone 1 in Figure 14 on page 79. The configuration is similar to the one for Zone1-SI-A, with the following exceptions:

- The management IP address is different.

- The default gateway goes to firewall FW2's interface with the ServerIron ADX. (The default gateway for Zone1-SI-A goes to FW1's interface with that ServerIron ADX.)

- The priority is set to 1 instead of 255. The lower priority makes this ServerIron ADX the standby ServerIron ADX by default.

- The paths are different due to the ServerIron ADX's placement in the network. (However, like Zone1-SI-A, ServerIron ADX Zone1-SI-S has a path through each firewall to each of the ServerIron ADXs in the other zones, and has a path to its directly attached router.)

```
ServerIronADX(config)# hostname Zone1-SI-S
Zone1-SI-S(config)# ip address 209.157.24.14 255.255.255.0
Zone1-SI-S(config)# ip default-gateway 209.157.24.254
Zone1-SI-S(config)# no span
Zone1-SI-S(config)# server router-ports 5
Zone1-SI-S(config)# server fw-port 9
Zone1-SI-S(config)# trunk switch ethernet 9 to 10
Zone1-SI-S(config)# trunk deploy
Zone1-SI-S(config)# vlan 10 by port
Zone1-SI-S(config-vlan-10)# untagged 9 to 10
Zone1-SI-S(config-vlan-10)# exit
Zone1-SI-S(config)# vlan 1
Zone1-SI-S(config-vlan-1)# always-active
Zone1-SI-S(config-vlan-1)# exit
Zone1-SI-S(config)# server fw-name FW1 209.157.24.1
Zone1-SI-S(config-rs-FW1)# exit
Zone1-SI-S(config)# server fw-name FW2 209.157.24.254
Zone1-SI-S(config-rs-FW2)# exit
Zone1-SI-S(config)# access-list 2 permit 209.157.25.0 0.0.0.255
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-S(config-fw-2)# fw-name FW1
Zone1-SI-S(config-fw-2)# fw-name FW2
Zone1-SI-S(config-fw-2)# l2-fwall
Zone1-SI-S(config-fw-2)# sym-priority 1
Zone1-SI-S(config-fw-2)# fwall-info 1 16 209.157.23.11 209.157.24.1
Zone1-SI-S(config-fw-2)# fwall-info 2 16 209.157.23.12 209.157.24.1
Zone1-SI-S(config-fw-2)# fwall-info 3 1 209.157.23.11 209.157.24.254
Zone1-SI-S(config-fw-2)# fwall-info 4 1 209.157.23.12 209.157.24.254
Zone1-SI-S(config-fw-2)# fwall-info 5 16 209.157.25.15 209.157.24.1
Zone1-SI-S(config-fw-2)# fwall-info 6 16 209.157.25.16 209.157.24.1
Zone1-SI-S(config-fw-2)# fwall-info 7 1 209.157.25.15 209.157.24.254
Zone1-SI-S(config-fw-2)# fwall-info 8 1 209.157.25.16 209.157.24.254
Zone1-SI-S(config-fw-2)# fwall-info 9 5 209.157.24.251 209.157.24.251
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# vlan 1
Zone1-SI-S(config-vlan-1)# static-mac-address abcd.5200.348d ethernet 1 priority
1 router-type
Zone1-SI-S(config-vlan-1)# static-mac-address abcd.5200.0b50 ethernet 16 priority
1 router-type
```

```
Zone1-SI-S(config-vlan-1)# exit
Zone1-SI-S(config)# write memory
Zone1-SI-S(config)# exit
Zone1-SI-S# reload
```

Commands on Zone2-SI-A in zone 2

The following commands configure ServerIron ADX "Zone2-SI-A" on the left side of zone 2 in Figure 14 on page 79. The configuration is similar to the one for the active ServerIron ADX in zone 1, with the following exceptions:

- The management IP address is different.

- The default gateway goes to a different interface on FW1.

- The paths are different due to the ServerIron ADX's placement in the network. (However, like Zone1-SI-A and Zone1-SI-S, ServerIron ADX Zone1-SI-S has a path through each firewall to each of the ServerIron ADXs in the other zones, and has a path to its directly attached router.)

- Only one ACL and zone definition are configured for zone 3. Because this ServerIron ADX is in zone 2, the configuration does not include an ACL and zone definition for the zone. This ServerIron ADX also does not contain an ACL or zone definition for zone 1. As a result, by default, this ServerIron ADX forwards packets that are not addressed to the ServerIron ADX's own sub-net, or to a sub-net in zone 3, to zone 1.

```
ServerIronADX(config)# hostname Zone2-SI-A
Zone2-SI-A(config)# ip address 209.157.24.15 255.255.255.0
Zone2-SI-A(config)# ip default-gateway 209.157.25.1
Zone2-SI-A(config)# no span
Zone2-SI-A(config)# server router-ports 5
Zone2-SI-A(config)# server fw-port 9
Zone2-SI-A(config)# trunk switch ethernet 9 to 10
Zone2-SI-A(config)# trunk deploy
Zone2-SI-A(config)# vlan 10 by port
Zone2-SI-A(config-vlan-10)# untagged 9 to 10
Zone2-SI-A(config-vlan-10)# exit
Zone2-SI-A(config)# vlan 1
Zone2-SI-A(config-vlan-1)# always-active
Zone2-SI-A(config-vlan-1)# exit
Zone2-SI-A(config)# server fw-name FW1 209.157.25.1
Zone2-SI-A(config-rs-FW1)# exit
Zone2-SI-A(config)# server fw-name FW2 209.157.25.254
Zone2-SI-A(config-rs-FW2)# exit
Zone2-SI-A(config)# access-list 3 permit 209.157.23.0 0.0.0.255
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fwall-zone Zone3 3 3
Zone2-SI-A(config-fw-2)# fw-name FW1
Zone2-SI-A(config-fw-2)# fw-name FW2
Zone2-SI-A(config-fw-2)# l2-fwall
Zone2-SI-A(config-fw-2)# sym-priority 255
Zone2-SI-A(config-fw-2)# fwall-info 1 1 209.157.23.11 209.157.25.1
Zone2-SI-A(config-fw-2)# fwall-info 2 1 209.157.23.12 209.157.25.1
Zone2-SI-A(config-fw-2)# fwall-info 3 1 209.157.24.13 209.157.25.1
Zone2-SI-A(config-fw-2)# fwall-info 4 1 209.157.24.14 209.157.25.1
Zone2-SI-A(config-fw-2)# fwall-info 5 16 209.157.23.11 209.157.25.254
Zone2-SI-A(config-fw-2)# fwall-info 6 16 209.157.23.12 209.157.25.254
Zone2-SI-A(config-fw-2)# fwall-info 7 16 209.157.24.13 209.157.25.254
Zone2-SI-A(config-fw-2)# fwall-info 8 16 209.157.24.14 209.157.25.254
Zone2-SI-A(config-fw-2)# fwall-info 9 5 209.157.25.200 209.157.25.200
Zone2-SI-A(config-fw-2)# exit
```

```
Zone2-SI-A(config)# vlan 1
Zone2-SI-A(config-vlan-1)# static-mac-address abcd.5200.348b ethernet 1 priority
1 router-type
Zone2-SI-A(config-vlan-1)# static-mac-address abcd.5200.0b4e ethernet 16 priority
1 router-type
Zone2-SI-A(config-vlan-1)# exit
Zone2-SI-A(config)# write memory
Zone2-SI-A(config)# exit
Zone2-SI-A# reload
```

Commands on Zone2-SI-S in zone 2

The following commands configure ServerIron ADX "Zone2-SI-S" on the right side of zone 2 in
Figure 14 on page 79.

```
ServerIron ADX(config)# hostname Zone2-SI-S
Zone2-SI-S(config)# ip address 209.157.25.16 255.255.255.0
Zone2-SI-S(config)# ip default-gateway 209.157.25.254
Zone2-SI-S(config)# no span
Zone2-SI-S(config)# server router-ports 5
Zone2-SI-S(config)# server fw-port 9
Zone2-SI-S(config)# trunk switch ethernet 9 to 10
Zone2-SI-S(config)# trunk deploy
Zone2-SI-S(config)# vlan 10 by port
Zone2-SI-S(config-vlan-10)# untagged 9 to 10
Zone2-SI-S(config-vlan-10)# exit
Zone2-SI-S(config)# vlan 1
Zone2-SI-S(config-vlan-1)# always-active
Zone2-SI-S(config-vlan-1)# exit
Zone2-SI-S(config)# server fw-name FW1 209.157.25.1
Zone2-SI-S(config-rs-FW1)# exit
Zone2-SI-S(config)# server fw-name FW2 209.157.25.254
Zone2-SI-S(config-rs-FW2)# exit
Zone2-SI-S(config)# access-list 3 permit 209.157.23.0 0.0.0.255
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fwall-zone Zone3 3 3
Zone2-SI-S(config-fw-2)# fw-name FW1
Zone2-SI-S(config-fw-2)# fw-name FW2
Zone2-SI-S(config-fw-2)# l2-fwall
Zone2-SI-S(config-fw-2)# sym-priority 1
Zone2-SI-S(config-fw-2)# fwall-info 1 16 209.157.23.11 209.157.25.1
Zone2-SI-S(config-fw-2)# fwall-info 2 16 209.157.23.12 209.157.25.1
Zone2-SI-S(config-fw-2)# fwall-info 3 16 209.157.24.13 209.157.25.1
Zone2-SI-S(config-fw-2)# fwall-info 4 16 209.157.24.14 209.157.25.1
Zone2-SI-S(config-fw-2)# fwall-info 5 1 209.157.23.11 209.157.25.254
Zone2-SI-S(config-fw-2)# fwall-info 6 1 209.157.23.12 209.157.25.254
Zone2-SI-S(config-fw-2)# fwall-info 7 1 209.157.24.13 209.157.25.254
Zone2-SI-S(config-fw-2)# fwall-info 8 1 209.157.24.14 209.157.25.254
Zone2-SI-S(config-fw-2)# fwall-info 9 5 209.157.25.200 209.157.25.201
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# vlan 1
Zone2-SI-S(config-vlan-1)# static-mac-address abcd.5200.348b ethernet 1 priority
1 router-type
Zone2-SI-S(config-vlan-1)# static-mac-address abcd.5200.0b4e ethernet 16 priority
1 router-type
Zone2-SI-S(config-vlan-1)# exit
Zone2-SI-S(config)# write memory
Zone2-SI-S(config)# exit
Zone2-SI-S# reload
```

Commands on Zone3-SI-A in zone 3

The following commands configure ServerIron ADX "Zone3-SI-A" on the left side of zone 3 in
Figure 14 on page 79.

```
ServerIronADX(config)# hostname Zone3-SI-A
Zone3-SI-A(config)# ip address 209.157.23.11 255.255.255.0
Zone3-SI-A(config)# ip default-gateway 209.157.23.1
Zone3-SI-A(config)# no span
Zone3-SI-A(config)# server router-ports 5
Zone3-SI-A(config)# server fw-port 9
Zone3-SI-A(config)# trunk switch ethernet 9 to 10
Zone3-SI-A(config)# trunk deploy
Zone3-SI-A(config)# vlan 10 by port
Zone3-SI-A(config-vlan-10)# untagged 9 to 10
Zone3-SI-A(config-vlan-10)# exit
Zone3-SI-A(config)# vlan 1
Zone3-SI-A(config-vlan-1)# always-active
Zone3-SI-A(config-vlan-1)# exit
Zone3-SI-A(config)# server fw-name FW1 209.157.23.1
Zone3-SI-A(config-rs-FW1)# exit
Zone3-SI-A(config)# server fw-name FW2 209.157.23.254
Zone3-SI-A(config-rs-FW2)# exit
Zone3-SI-A(config)# access-list 2 permit 209.157.25.0 0.0.0.255
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fwall-zone Zone2 2 2
Zone3-SI-A(config-fw-2)# fw-name FW1
Zone3-SI-A(config-fw-2)# fw-name FW2
Zone3-SI-A(config-fw-2)# l2-fwall
Zone3-SI-A(config-fw-2)# sym-priority 255
Zone3-SI-A(config-fw-2)# fwall-info 1 1 209.157.24.13 209.157.23.1
Zone3-SI-A(config-fw-2)# fwall-info 2 1 209.157.24.14 209.157.23.1
Zone3-SI-A(config-fw-2)# fwall-info 3 16 209.157.24.13 209.157.23.254
Zone3-SI-A(config-fw-2)# fwall-info 4 16 209.157.24.14 209.157.23.254
Zone3-SI-A(config-fw-2)# fwall-info 5 1 209.157.25.15 209.157.23.1
Zone3-SI-A(config-fw-2)# fwall-info 6 1 209.157.25.16 209.157.23.1
Zone3-SI-A(config-fw-2)# fwall-info 7 16 209.157.25.15 209.157.23.254
Zone3-SI-A(config-fw-2)# fwall-info 8 16 209.157.25.16 209.157.23.254
Zone3-SI-A(config-fw-2)# fwall-info 9 5 209.157.23.15 209.157.23.15
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# vlan 1
Zone3-SI-A(config-vlan-1)# static-mac-address abcd.5200.3489 ethernet 1 priority
1 router-type
Zone3-SI-A(config-vlan-1)# static-mac-address abcd.5200.0b4c ethernet 16 priority
1 router-type
Zone3-SI-A(config-vlan-1)# exit
Zone3-SI-A(config)# write memory
Zone3-SI-A(config)# exit
Zone3-SI-A# reload
```

Commands on Zone3-SI-S in zone 3

The following commands configure ServerIron ADX "Zone3-SI-S" on the right side of zone 3 in
Figure 14 on page 79.

```
ServerIronADX(config)# hostname Zone3-SI-S
Zone3-SI-S(config)# ip address 209.157.23.12 255.255.255.0
Zone3-SI-S(config)# ip default-gateway 209.157.23.254
Zone3-SI-S(config)# no span
Zone3-SI-S(config)# server router-ports 5
Zone3-SI-S(config)# server fw-port 9
Zone3-SI-S(config)# trunk switch ethernet 9 to 10
Zone3-SI-S(config)# trunk deploy
Zone3-SI-S(config)# vlan 10 by port
Zone3-SI-S(config-vlan-10)# untagged 9 to 10
Zone3-SI-S(config-vlan-10)# exit
Zone3-SI-S(config)# vlan 1
Zone3-SI-S(config-vlan-1)# always-active
Zone3-SI-S(config-vlan-1)# exit
Zone3-SI-S(config)# server fw-name FW1 209.157.23.1
Zone3-SI-S(config-rs-FW1)# exit
Zone3-SI-S(config)# server fw-name FW2 209.157.23.254
Zone3-SI-S(config-rs-FW2)# exit
Zone3-SI-S(config)# access-list 2 permit 209.157.25.0 0.0.0.255
Zone3-SI-S(config)# server fw-group 2
Zone3-SI-S(config-fw-2)# fwall-zone Zone2 2 2
Zone3-SI-S(config-fw-2)# fw-name FW1
Zone3-SI-S(config-fw-2)# fw-name FW2
Zone3-SI-S(config-fw-2)# l2-fwall
Zone3-SI-S(config-fw-2)# sym-priority 1
Zone3-SI-S(config-fw-2)# fwall-info 1 16 209.157.24.13 209.157.23.1
Zone3-SI-S(config-fw-2)# fwall-info 2 16 209.157.24.14 209.157.23.1
Zone3-SI-S(config-fw-2)# fwall-info 3 1 209.157.24.13 209.157.23.254
Zone3-SI-S(config-fw-2)# fwall-info 4 1 209.157.24.14 209.157.23.254
Zone3-SI-S(config-fw-2)# fwall-info 5 16 209.157.25.15 209.157.23.1
Zone3-SI-S(config-fw-2)# fwall-info 6 16 209.157.25.16 209.157.23.1
Zone3-SI-S(config-fw-2)# fwall-info 7 1 209.157.25.15 209.157.23.1
Zone3-SI-S(config-fw-2)# fwall-info 8 1 209.157.25.16 209.157.23.254
Zone3-SI-S(config-fw-2)# fwall-info 9 5 209.157.23.15 209.157.23.15
Zone3-SI-S(config-fw-2)# exit
Zone3-SI-S(config)# vlan 1
Zone3-SI-S(config-vlan-1)# static-mac-address abcd.5200.3489 ethernet 1
priority 1 router-type
Zone3-SI-S(config-vlan-1)# static-mac-address abcd.5200.0b4c ethernet 16
priority 1 router-type
Zone3-SI-S(config-vlan-1)# exit
Zone3-SI-S(config)# write memory
Zone3-SI-S(config)# exit
Zone3-SI-S# reload
```

IronClad FWLB configurations require each ServerIron ADX in an active-standby pair to have a link
to each of the firewalls for which the ServerIron ADXs are providing load balancing.

If the firewalls are multi-homed (allow more than one connection on each side of the protected network), then it is possible to connect each ServerIron ADX to all the firewalls directly. Figure 15 shows an example of this type of configuration.

FIGURE 15   IronClad FWLB configuration with multi-homed firewalls
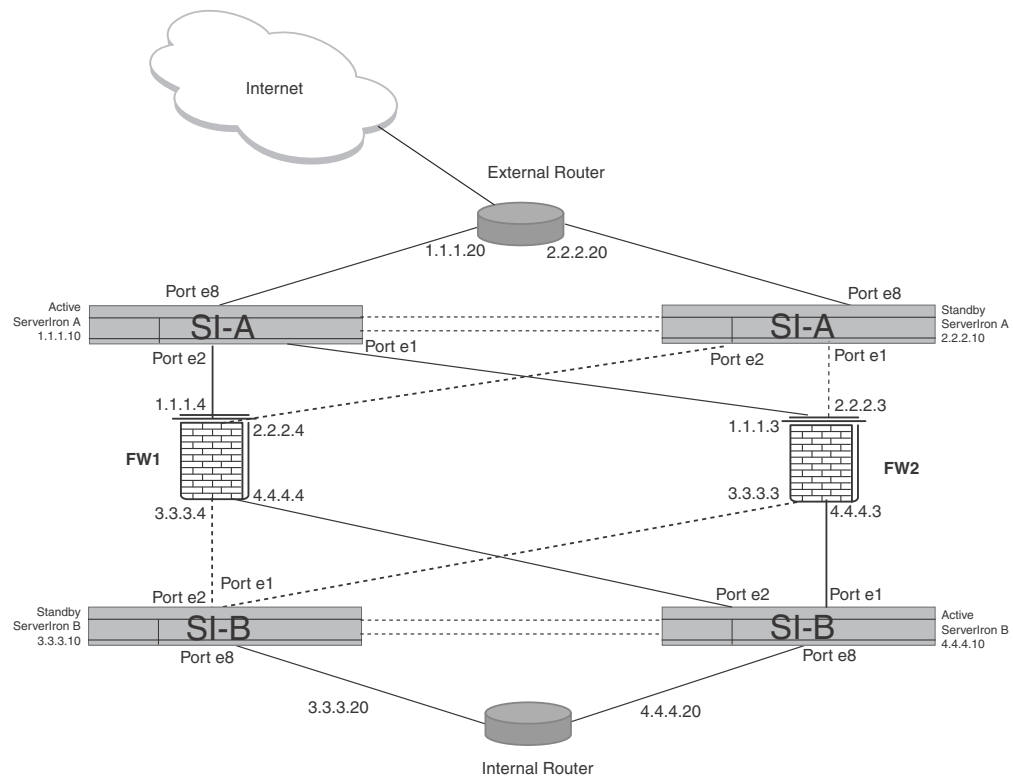
In this example, each firewall has four interfaces. Each interface goes to a ServerIron ADX.

NOTE

If the firewalls are not multi-homed, you must use additional devices, typically Layer 2 switches, to provide the redundant links. Figure 15 shows an example of an IronClad FWLB configuration that uses Layer 2 switches to provide multi-homing between the ServerIron ADXs and firewalls.

Configuration examples with Layer 3 routing

This section shows examples of commonly used ServerIron ADX multizone FWLB deployments with Layer 3 configurations. The ServerIron ADXs in these examples perform Layer 3 routing in addition to Layer 2 and Layer 4–7 switching.

Generally, the steps for configuring Layer 4–7 features on a ServerIron ADX running Layer 3 are similar to the steps on a ServerIron ADX that is not running Layer 3. The examples focus on the Layer 3 aspects of the configurations.

This section contains the following configuration examples:

-
-

NOTE
The multizone FWLB configurations shown in these examples are the ones that are supported. If you need to use the ServerIron ADX's Layer 3 routing support in a FWLB configuration that is not shown, contact Brocade.

Multizone FWLB with one sub-net and one virtual routing interface

Multizone FWLB allows you to configure ServerIron ADXs to forward packets based on the destination zone. For example, if your network consists of an Internet side, an internal side, and a Demilitarized Zone (DMZ) in between, you can configure ServerIron ADXs to forward packets through the firewalls to the correct zone.

When you configure multizone FWLB, you first identify a zone by configuring standard ACLs. An ACL specifies the IP addresses (or address ranges) within the zone. When you configure the firewall group parameters, you add the zones and define them by associating the ACLs with them. Each zone consists of a zone number, an optional name, and a standard IP ACL that specifies the IP addresses contained in the zone.

Figure 16 shows an example of a multizone configuration for three zones:

- Zone 1 – The default zone. All sub-nets that you do not configure to be members of the other zones are by default members of zone 1. Generally, the default zone is on the public (non-secure) side of the firewalls.
- Zone 2 – A secured zone containing two application servers.
- Zone 3 – Another secured zone containing an additional application server.

The ServerIron ADXs in zone 1 perform FWLB for traffic between zone 1 and zones 2 and 3.

FIGURE 16   Multizone FWLB with one sub-net and one virtual routing interface
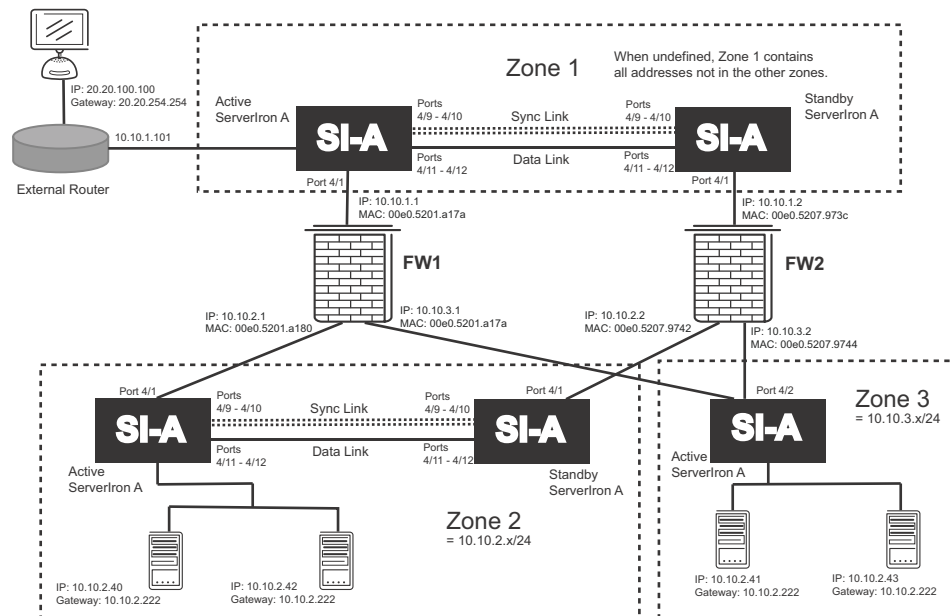
This configuration example also uses SLB. The application servers connected to the ServerIron ADXs in zones 2 and 3 are configured on the ServerIron ADXs as real servers and bound to a virtual IP. The ServerIron ADXs in zone 1 load balance client requests for the servers in zones 2 and 3, in addition to load balancing the traffic to the firewalls. FWLB-to-SLB and SLB-to-FWLB are used in this configuration. FWLB-to-SLB enables the ServerIron ADXs in zones 2 and 3 to learn the firewall from which a client request is received and send the server reply back through the same firewall. SLB-to-FWLB on the ServerIron ADXs in zone 1 performs FWLB for traffic directed toward the real servers connected to the ServerIron ADXs in zones 2 and 3.

Commands on zone 1's active ServerIron ADX (Zone1-SI-A)

The following commands change the CLI to the global CONFIG level, and then change the host name to "Zone1-SI-A".

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone1-SI-A
```

The following commands enable the always-active feature and disable the Spanning Tree Protocol (STP) in VLAN 1, which contains the ports that will carry the FWLB traffic.

```
Zone1-SI-A(config)# vlan 1
Zone1-SI-A(config-vlan-1)# always-active
Zone1-SI-A(config-vlan-1)# no spanning-tree
```

The following commands configure a virtual routing interface on VLAN 1 (the default VLAN), and then configure an IP address on the interface. The virtual routing interface is associated with all the ports in the VLAN.

```
Zone1-SI-A(config-vlan-1)# router-interface ve 1
Zone1-SI-A(config-vlan-1)# exit
Zone1-SI-A(config)# interface ve 1
Zone1-SI-A(config-ve-1)# ip address 10.10.1.111 255.255.255.0
Zone1-SI-A(config-ve-1)# exit
```

The following command configures an IP default route. The next hop for this route is the ServerIron ADX's interface with firewall FW1.

```
Zone1-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
```

The following command disables ICMP redirect messages. This command disables the messages but the ServerIron ADX still forwards misdirected traffic to the appropriate router.

```
Zone1-SI-A(config)# no ip icmp redirects
```

The following commands configure the synchronization link between this ServerIron ADX and ServerIron ADX Zone1-SI-B. For redundancy, the link is configured on a trunk group.

```
Zone1-SI-A(config)# vlan 10
Zone1-SI-A(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone1-SI-A(config-vlan-10)# exit
Zone1-SI-A(config)# trunk switch ethernet 4/9 to 4/10
Zone1-SI-A(config)# trunk deploy
Zone1-SI-A(config)# server fw-port 4/9
```

The following commands configure the data link connecting this ServerIron ADX to its partner, Zone1-SI-B. For redundancy, the link is configured as a two-port trunk group.

```
Zone1-SI-A(config)# trunk switch ethernet 4/11 to 4/12
Zone1-SI-A(config)# trunk deploy
Zone1-SI-A(config)# server partner-ports ethernet 4/11
Zone1-SI-A(config)# server partner-ports ethernet 4/12
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# l2-fwall
Zone1-SI-A(config-fw-2)# exit
```

The following commands add the firewalls. Three application ports (HTTP, FTP, and SNMP) are configured on each of the firewalls. The **no-health-check** parameter disables the Layer 4 health check for the specified application.

```
Zone1-SI-A(config)# server fw-name fw1 10.10.1.1
Zone1-SI-A(config-rs-fw1)# port http
Zone1-SI-A(config-rs-fw1)# port http no-health-check
Zone1-SI-A(config-rs-fw1)# port ftp
Zone1-SI-A(config-rs-fw1)# port ftp no-health-check
Zone1-SI-A(config-rs-fw1)# port snmp
Zone1-SI-A(config-rs-fw1)# port snmp no-health-check
Zone1-SI-A(config-rs-fw1)# exit
Zone1-SI-A(config)# server fw-name fw2 10.10.1.2
Zone1-SI-A(config-rs-fw2)# port http
Zone1-SI-A(config-rs-fw2)# port http no-health-check
Zone1-SI-A(config-rs-fw2)# port ftp
Zone1-SI-A(config-rs-fw2)# port ftp no-health-check
Zone1-SI-A(config-rs-fw2)# port snmp
Zone1-SI-A(config-rs-fw2)# port snmp no-health-check
Zone1-SI-A(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group (always group 2). The firewall group contains all the ports in VLAN 1 (the default VLAN).

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fw-name fw1
Zone1-SI-A(config-fw-2)# fw-name fw2
```

The following command enables the active-active mode. For details about configuring this command, refer to "Enabling the active-active mode" on page 48.

```
Zone1-SI-A(config-fw-2)# sym-priority 255
```

The following commands add the paths through the firewalls to the ServerIron ADXs in zones 2 and 3. In addition, static MAC entries are added for the firewall interfaces. Static MAC entries are required in this type of configuration, in which one sub-net and one virtual routing interface are used.

NOTE
The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
Zone1-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 2 4/11 10.10.2.222 10.10.1.2
Zone1-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 4 4/11 10.10.2.223 10.10.1.2
Zone1-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.3.111 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 6 4/11 10.10.3.111 10.10.1.2
Zone1-SI-A(config-fw-2)# exit
Zone1-SI-A(config)# vlan 1
Zone1-SI-A(config-vlan-1)# static-mac-address 00e0.5201.a17a ethernet 4/1
priority 1 router-type
Zone1-SI-A(config-vlan-1)# static-mac-address 00e0.5207.973c ethernet 4/11
priority 1 router-type
Zone1-SI-A(config-vlan-1)# exit
```

The following commands set the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. For example, the ServerIron ADX will load balance HTTP requests based on the firewall that has fewer HTTP session entries in the ServerIron ADX session table.

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone1-SI-A(config-fw-2)# exit
```

The following command configures a standard IP ACL for the IP addresses in one of the zones this ServerIron ADX is not in. In this configuration, only one zone definition is required on each ServerIron ADX, including Zone1-SI-A and Zone1-SI-S. Because the active Zone 1 ServerIron ADX is already in zone 1, the ServerIron ADX will forward packets either to the active ServerIron ADX in zone 2 or to the only other active ServerIron ADX that is not in zone 2. In this case, the other active ServerIron ADX is in zone 3. Thus, if ServerIron ADX Zone1-SI-A receives a packet that is not addressed to the sub-net Zone1-SI-A is in, and is not addressed to a sub-net in zone 2, the ServerIron ADX assumes that the packet is for an address in the other zone, zone 3. The ServerIron ADX forwards the packet to the ServerIron ADX in zone 3.

The command configures an ACL for the addresses in zone 2, which contains addresses in the 10.10.2.x/24 sub-net. The "0.0.0.255" values indicate the significant bits in the IP address you specify. In this case, all bits except the ones in the last node of the address are significant.

```
Zone1-SI-A(config)# access-list 2 permit 10.10.2.0 0.0.0.255
```

The following commands configure the zone parameters. To configure a zone, specify a name for the zone, and then a zone number (from 1 through 10), followed by the number of the ACL that specifies the IP addresses in the zone. In this example, the ACL numbers and zone numbers are the same, but this is not required.

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-A(config-fw-2)# exit
```

The following commands configure the SLB information. Each of the servers in zones 2 and 3 is added as a real server, and then the servers are bound to a virtual IP. The servers are added using the **server remote-name** command instead of the **server real-name** command because the servers are not directly connected to the ServerIron ADX. Instead, they are connected to the ServerIron ADX through other routers (in this case, the firewalls).

```
Zone1-SI-A(config)# server remote-name web1 10.10.2.40
Zone1-SI-A(config-rs-web1)# port http
Zone1-SI-A(config-rs-web1)# exit
Zone1-SI-A(config)# server remote-name web2 10.10.2.42
Zone1-SI-A(config-rs-web2)# port http
Zone1-SI-A(config-rs-web2)# exit
Zone1-SI-A(config)# server remote-name web3 10.10.3.41
Zone1-SI-A(config-rs-web3)# port http
Zone1-SI-A(config-rs-web3)# exit
Zone1-SI-A(config)# server remote-name web4 10.10.3.43
Zone1-SI-A(config-rs-web4)# port http
Zone1-SI-A(config-rs-web4)# exit
Zone1-SI-A(config)# server virtual www.web.com 10.10.1.10
Zone1-SI-A(config-vs-www.web.com)# port http
Zone1-SI-A(config-vs-www.web.com)# bind http web1 http web2 http web3 http web4
http
Zone1-SI-A(config-vs-www.web.com)# exit
```

The following command enables SLB-to-FWLB.

```
Zone1-SI-A(config)# server slb-fw
```

The following command saves the configuration changes to the startup-config file.

```
Zone1-SI-A(config)# write memory
```

Commands on zone 1's standby ServerIron ADX (Zone1-SI-S)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone1-SI-S
Zone1-SI-S(config)# vlan 1
Zone1-SI-S(config-vlan-1)# always-active
Zone1-SI-S(config-vlan-1)# no spanning-tree
Zone1-SI-S(config-vlan-1)# router-interface ve 1
Zone1-SI-S(config-vlan-1)# exit
Zone1-SI-S(config)# interface ve 1
Zone1-SI-S(config-ve-1)# ip address 10.10.1.112 255.255.255.0
Zone1-SI-S(config-ve-1)# exit
Zone1-SI-S(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.2
Zone1-SI-S(config)# no ip icmp redirects
Zone1-SI-S(config)# vlan 10
Zone1-SI-S(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone1-SI-S(config-vlan-10)# exit
Zone1-SI-S(config)# trunk switch ethernet 4/9 to 4/10
```

```
Zone1-SI-S(config)# trunk deploy
Zone1-SI-S(config)# server fw-port 4/9
Zone1-SI-S(config)# trunk switch ethernet 4/11 to 4/12
Zone1-SI-S(config)# trunk deploy
Zone1-SI-S(config)# server partner-ports ethernet 4/11
Zone1-SI-S(config)# server partner-ports ethernet 4/12
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# l2-fwall
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# server fw-name fw1 10.10.1.1
Zone1-SI-S(config-rs-fw1)# port http
Zone1-SI-S(config-rs-fw1)# port http no-health-check
Zone1-SI-S(config-rs-fw1)# port ftp
Zone1-SI-S(config-rs-fw1)# port ftp no-health-check
Zone1-SI-S(config-rs-fw1)# port snmp
Zone1-SI-S(config-rs-fw1)# port snmp no-health-check
Zone1-SI-S(config-rs-fw1)# exit
Zone1-SI-S(config)# server fw-name fw2 10.10.1.2
Zone1-SI-S(config-rs-fw2)# port http
Zone1-SI-S(config-rs-fw2)# port http no-health-check
Zone1-SI-S(config-rs-fw2)# port ftp
Zone1-SI-S(config-rs-fw2)# port ftp no-health-check
Zone1-SI-S(config-rs-fw2)# port snmp
Zone1-SI-S(config-rs-fw2)# port snmp no-health-check
Zone1-SI-S(config-rs-fw2)# exit
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# fw-name fw1
Zone1-SI-S(config-fw-2)# fw-name fw2
Zone1-SI-S(config-fw-2)# sym-priority 1
Zone1-SI-S(config-fw-2)# fwall-info 1 4/11 10.10.2.222 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 2 4/1 10.10.2.222 10.10.1.2
Zone1-SI-S(config-fw-2)# fwall-info 3 4/11 10.10.2.223 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 4 4/1 10.10.2.223 10.10.1.2
Zone1-SI-S(config-fw-2)# fwall-info 5 4/11 10.10.3.111 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 6 4/1 10.10.3.111 10.10.1.2
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# vlan 1
Zone1-SI-S(config-vlan-1)# static-mac-address 00e0.5201.a17a ethernet 4/11
priority 1 router-type
Zone1-SI-S(config-vlan-1)# static-mac-address 00e0.5207.973c ethernet 4/1
priority 1 router-type
Zone1-SI-S(config-vlan-1)# exit
Zone1-SI-S(config-fw-2)# server fw-group 2
Zone1-SI-S(config-fw-2)# fw-predictor per-service-least-conn
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# access-list 2 permit 10.10.2.0 0.0.0.255
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# server remote-name web1 10.10.2.40
Zone1-SI-S(config-rs-web1)# port http
Zone1-SI-S(config-rs-web1)# exit
Zone1-SI-S(config)# server remote-name web2 10.10.2.42
Zone1-SI-S(config-rs-web2)# port http
Zone1-SI-S(config-rs-web2)# exit
Zone1-SI-S(config)# server remote-name web3 10.10.3.41
Zone1-SI-S(config-rs-web3)# port http
Zone1-SI-S(config-rs-web3)# exit
Zone1-SI-S(config)# server remote-name web4 10.10.3.43
Zone1-SI-S(config-rs-web4)# port http
```

```
Zone1-SI-S(config-rs-web4)# exit
Zone1-SI-S(config)# server virtual www.web.com 10.10.1.10
Zone1-SI-S(config-vs-www.web.com)# port http
Zone1-SI-S(config-vs-www.web.com)# bind http web1 http web2 http web3 http web4
http
Zone1-SI-S(config-vs-www.web.com)# exit
Zone1-SI-S(config)# server slb-fw
Zone1-SI-S(config)# write memory
```

Commands on zone 2's active ServerIron ADX (Zone2-SI-A)

The following commands configure ServerIron ADX Zone2-SI-A in zone 2. The configuration is similar to the configuration for ServerIron ADX Zone1-SI-A, except the ACL and zone information are for zone 3, and FWLB-to-SLB is enabled instead of SLB-to-FWLB.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone2-SI-A
Zone2-SI-A(config)# vlan 1
Zone2-SI-A(config-vlan-1)# always-active
Zone2-SI-A(config-vlan-1)# no spanning-tree
Zone2-SI-A(config-vlan-1)# router-interface ve 1
Zone2-SI-A(config-vlan-1)# exit
Zone2-SI-A(config)# interface ve 1
Zone2-SI-A(config-ve-1)# ip address 10.10.2.222 255.255.255.0
Zone2-SI-A(config-ve-1)# exit
Zone2-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.1
Zone2-SI-A(config)# no ip icmp redirects
Zone2-SI-A(config)# vlan 10
Zone2-SI-A(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone2-SI-A(config-vlan-10)# exit
Zone2-SI-A(config)# trunk switch ethernet 4/9 to 4/10
Zone2-SI-A(config)# trunk deploy
Zone2-SI-A(config)# server fw-port 4/9
Zone2-SI-A(config)# trunk switch ethernet 4/11 to 4/12
Zone2-SI-A(config)# trunk deploy
Zone2-SI-A(config)# server partner-ports ethernet 4/11
Zone2-SI-A(config)# server partner-ports ethernet 4/12
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# l2-fwall
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# server fw-name fw1 10.10.2.1
Zone2-SI-A(config-rs-fw1)# port http
Zone2-SI-A(config-rs-fw1)# port http no-health-check
Zone2-SI-A(config-rs-fw1)# port ftp
Zone2-SI-A(config-rs-fw1)# port ftp no-health-check
Zone2-SI-A(config-rs-fw1)# port snmp
Zone2-SI-A(config-rs-fw1)# port snmp no-health-check
Zone2-SI-A(config-rs-fw1)# exit
Zone2-SI-A(config)# server fw-name fw2 10.10.2.2
Zone2-SI-A(config-rs-fw2)# port http
Zone2-SI-A(config-rs-fw2)# port http no-health-check
Zone2-SI-A(config-rs-fw2)# port ftp
Zone2-SI-A(config-rs-fw2)# port ftp no-health-check
Zone2-SI-A(config-rs-fw2)# port snmp
Zone2-SI-A(config-rs-fw2)# port snmp no-health-check
Zone2-SI-A(config-rs-fw2)# exit
```

```
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fw-name fw1
Zone2-SI-A(config-fw-2)# fw-name fw2
Zone2-SI-A(config-fw-2)# sym-priority 255
Zone2-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 2 4/11 10.10.1.111 10.10.2.2
Zone2-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 4 4/11 10.10.1.112 10.10.2.2
Zone2-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.3.111 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 6 4/11 10.10.3.111 10.10.2.2
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# vlan 1
Zone2-SI-A(config-vlan-1)# static-mac-address 00e0.5201.a180 ethernet 4/1
priority 1 router-type
Zone2-SI-A(config-vlan-1)# static-mac-address 00e0.5207.9742 ethernet 4/11
priority 1 router-type
Zone2-SI-A(config-vlan-1)# exit
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# access-list 3 permit 10.10.3.0 0.0.0.255
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fwall-zone zone3 3 3
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# server real-name rs1 10.10.2.40
Zone2-SI-A(config-rs-rs1)# port http
Zone2-SI-A(config-rs-rs1)# exit
Zone2-SI-A(config)# server real-name rs1 10.10.2.42
Zone2-SI-A(config-rs-rs2)# port http
Zone2-SI-A(config-rs-rs2)# exit
Zone2-SI-A(config)# server virtual www.rs.com 10.10.2.10
Zone2-SI-A(config-vs-www.rs.com)# port http
Zone2-SI-A(config-vs-www.web.com)# bind http rs1 http rs2 http
Zone2-SI-A(config-vs-www.web.com)# exit
Zone2-SI-A(config)# server fw-slb
Zone2-SI-A(config)# write memory
```

Commands on zone 2's standby ServerIron ADX (Zone2-SI-S)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone2-SI-S
Zone2-SI-S(config)# vlan 1
Zone2-SI-S(config-vlan-1)# always-active
Zone2-SI-S(config-vlan-1)# no spanning-tree
Zone2-SI-S(config-vlan-1)# router-interface ve 1
Zone2-SI-S(config-vlan-1)# exit
Zone2-SI-S(config)# interface ve 1
Zone2-SI-S(config-ve-1)# ip address 10.10.2.223 255.255.255.0
Zone2-SI-S(config-ve-1)# exit
Zone2-SI-S(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.2
Zone2-SI-S(config)# no ip icmp redirects
Zone2-SI-S(config)# vlan 10
Zone2-SI-S(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone2-SI-S(config-vlan-10)# exit
Zone2-SI-S(config)# trunk switch ethernet 4/9 to 4/10
Zone2-SI-S(config)# server fw-port 4/9
Zone2-SI-S(config)# trunk switch ethernet 4/11 to 4/12
Zone2-SI-S(config)# server partner-ports ethernet 4/11
```

```
Zone2-SI-S(config)# server partner-ports ethernet 4/12
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# l2-fwall
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# server fw-name fw1 10.10.2.1
Zone2-SI-S(config-rs-fw1)# port http
Zone2-SI-S(config-rs-fw1)# port http no-health-check
Zone2-SI-S(config-rs-fw1)# port ftp
Zone2-SI-S(config-rs-fw1)# port ftp no-health-check
Zone2-SI-S(config-rs-fw1)# port snmp
Zone2-SI-S(config-rs-fw1)# port snmp no-health-check
Zone2-SI-S(config-rs-fw1)# exit
Zone2-SI-S(config)# server fw-name fw2 10.10.2.2
Zone2-SI-S(config-rs-fw2)# port http
Zone2-SI-S(config-rs-fw2)# port http no-health-check
Zone2-SI-S(config-rs-fw2)# port ftp
Zone2-SI-S(config-rs-fw2)# port ftp no-health-check
Zone2-SI-S(config-rs-fw2)# port snmp
Zone2-SI-S(config-rs-fw2)# port snmp no-health-check
Zone2-SI-S(config-rs-fw2)# exit
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fw-name fw1
Zone2-SI-S(config-fw-2)# fw-name fw2
Zone2-SI-S(config-fw-2)# sym-priority 1
Zone2-SI-S(config-fw-2)# fwall-info 1 4/11 10.10.1.111 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 2 4/1 10.10.1.111 10.10.2.2
Zone2-SI-S(config-fw-2)# fwall-info 3 4/11 10.10.1.112 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 4 4/1 10.10.1.112 10.10.2.2
Zone2-SI-S(config-fw-2)# fwall-info 5 4/11 10.10.3.111 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 6 4/1 10.10.3.111 10.10.2.2
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# vlan 1
Zone2-SI-S(config-vlan-1)# static-mac-address 00e0.5201.a180 ethernet 4/11
priority 1 router-type
Zone2-SI-S(config-vlan-1)# static-mac-address 00e0.5207.9742 ethernet 4/1
priority 1 router-type
Zone2-SI-S(config-vlan-1)# exit
Zone2-SI-S(config)# server group 2
Zone2-SI-S(config-fw-2)# fw-predictor per-service-least-conn
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# access-list 3 permit 10.10.3.0 0.0.0.255
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fwall-zone zone3 3 3
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# server real-name rs1 10.10.2.40
Zone2-SI-S(config-rs-rs1)# port http
Zone2-SI-S(config-rs-rs1)# exit
Zone2-SI-S(config)# server real-name rs1 10.10.2.42
Zone2-SI-S(config-rs-rs2)# port http
Zone2-SI-S(config-rs-rs2)# exit
Zone2-SI-S(config)# server virtual www.rs.com 10.10.2.10
Zone2-SI-S(config-vs-www.rs.com)# port http
Zone2-SI-S(config-vs-www.web.com)# bind http rs1 http rs2 http
Zone2-SI-S(config-vs-www.web.com)# exit
Zone2-SI-S(config)# server fw-slb
Zone2-SI-S(config)# write memory
```

Commands on zone 3's ServerIron ADX (Zone3-SI-A)

The following commands configure the ServerIron ADX in zone 3.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone3-SI-A
Zone3-SI-A(config)# vlan 1
Zone3-SI-A(config-vlan-1)# always-active
Zone3-SI-A(config-vlan-1)# no spanning-tree
Zone3-SI-A(config-vlan-1)# router-interface ve 1
Zone3-SI-A(config-vlan-1)# exit
Zone3-SI-A(config)# interface ve 1
Zone3-SI-A(config-ve-1)# ip address 10.10.3.111 255.255.255.0
Zone3-SI-A(config-ve-1)# exit
Zone3-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.3.1
Zone3-SI-A(config)# no ip icmp redirects
Zone3-SI-A(config)# server fw-name fw1 10.10.3.1
Zone3-SI-A(config-rs-fw1)# port http
Zone3-SI-A(config-rs-fw1)# port http no-health-check
Zone3-SI-A(config-rs-fw1)# port ftp
Zone3-SI-A(config-rs-fw1)# port ftp no-health-check
Zone3-SI-A(config-rs-fw1)# port snmp
Zone3-SI-A(config-rs-fw1)# port snmp no-health-check
Zone3-SI-A(config-rs-fw1)# exit
Zone3-SI-A(config)# server fw-name fw2 10.10.3.2
Zone3-SI-A(config-rs-fw2)# port http
Zone3-SI-A(config-rs-fw2)# port http no-health-check
Zone3-SI-A(config-rs-fw2)# port ftp
Zone3-SI-A(config-rs-fw2)# port ftp no-health-check
Zone3-SI-A(config-rs-fw2)# port snmp
Zone3-SI-A(config-rs-fw2)# port snmp no-health-check
Zone3-SI-A(config-rs-fw2)# exit
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fw-name fw1
Zone3-SI-A(config-fw-2)# fw-name fw2
Zone3-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 2 4/2 10.10.1.111 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 4 4/2 10.10.1.112 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.2.222 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 6 4/2 10.10.2.222 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 7 4/1 10.10.2.223 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 8 4/2 10.10.2.223 10.10.3.2
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# vlan 1
Zone3-SI-A(config-vlan-1)# static-mac-address 00e0.5201.a182 ethernet 4/1
priority 1 router-type
Zone3-SI-A(config-vlan-1)# static-mac-address 00e0.5207.9744 ethernet 4/2
priority 1 router-type
Zone3-SI-A(config-vlan-1)# exit
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# access-list 2 permit 10.10.2.0 0.0.0.255
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fwall-zone zone2 2 2
Zone3-SI-A(config-fw-2)# exit
```

```
Zone3-SI-A(config)# server real-name sr1 10.10.3.41
Zone3-SI-A(config-rs-sr1)# port http
Zone3-SI-A(config-rs-sr1)# exit
Zone3-SI-A(config)# server real-name sr2 10.10.3.43
Zone3-SI-A(config-rs-sr2)# port http
Zone3-SI-A(config-rs-sr2)# exit
Zone3-SI-A(config)# server virtual www.sr.com 10.10.3.10
Zone3-SI-A(config-vs-www.rs.com)# port http
Zone3-SI-A(config-vs-www.web.com)# bind http sr2 http sr1 http
Zone3-SI-A(config-vs-www.web.com)# exit
Zone3-SI-A(config)# server fw-slb
Zone3-SI-A(config)# write memory
```

Multizone FWLB with multiple sub-nets and multiple virtual routing interfaces

Figure 17 shows an example of a multizone FWLB configuration in which each ServerIron ADX is configured with multiple sub-nets and multiple virtual routing interfaces. The configuration is similar to the one in Figure 16 on page 93, but differs in the following ways:

- The ServerIron ADXs configured in active-active pairs have four port-based VLANs. VLAN 10 is for the synchronization link between the ServerIron ADXs. The default VLAN (VLAN 1) is not configured with a routing interface. VLANs 2 and 20 are configured with virtual routing interfaces.

- The ServerIron ADXs in zone 1 are configured with a static IP route to the sub-net that the external client is on.

- Static MAC entries are not required and thus are not included for the firewall interfaces.

- More than one standard IP ACL is configured on each ServerIron ADX, because more than one sub-net is a member of each zone.

FIGURE 17   Multizone FWLB with multiple sub-nets and multiple virtual routing interfaces
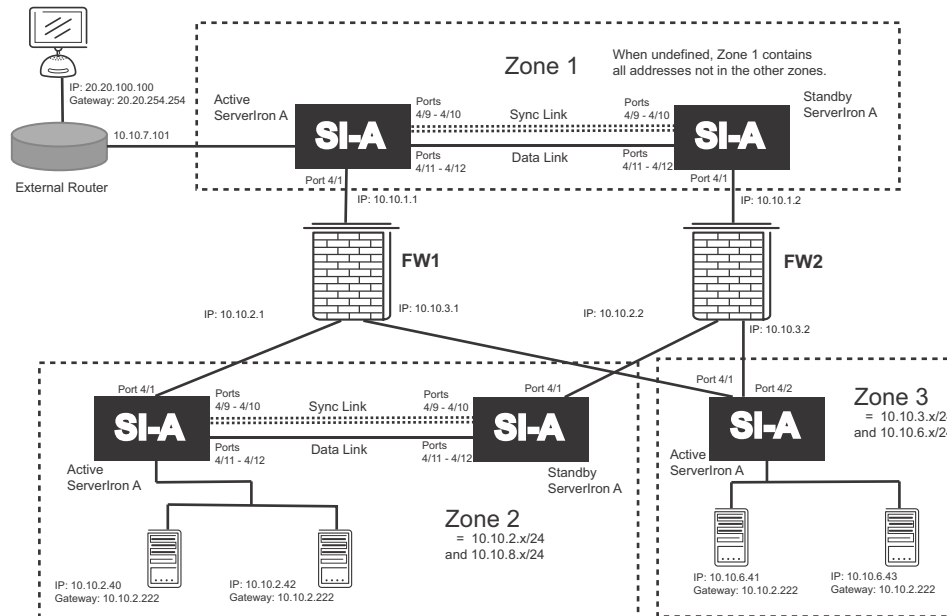
Commands on zone 1's active ServerIron ADX (Zone1-SI-A)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone1-SI-A
```

The following commands enable the always-active feature in VLAN 1.

```
Zone1-SI-A(config)# vlan 1
Zone1-SI-A(config-vlan-1)# always-active
Zone1-SI-A(config-vlan-1)# exit
```

The following commands configure VLAN 2 and virtual routing interface 1, for 10.10.1.111.

```
Zone1-SI-A(config)# vlan 2
Zone1-SI-A(config-vlan-2)# always-active
Zone1-SI-A(config-vlan-2)# tagged ethernet 4/11 to 4/12
Zone1-SI-A(config-vlan-2)# untagged ethernet 4/1 to 4/8
Zone1-SI-A(config-vlan-2)# router-interface ve 1
Zone1-SI-A(config-vlan-2)# exit
Zone1-SI-A(config)# interface ve 1
Zone1-SI-A(config-ve-1)# ip address 10.10.1.111 255.255.255.0
Zone1-SI-A(config-ve-1)# exit
```

The following commands configure VLAN 20 and virtual routing interface 2, for 10.10.7.101.

```
Zone1-SI-A(config)# vlan 20
Zone1-SI-A(config-vlan-20)# always-active
Zone1-SI-A(config-vlan-20)# tagged ethernet 4/11 to 4/12
Zone1-SI-A(config-vlan-20)# untagged ethernet 4/13 to 4/24
Zone1-SI-A(config-vlan-20)# router-interface ve 2
Zone1-SI-A(config-vlan-20# exit
Zone1-SI-A(config)# interface ve 2
```

```
Zone1-SI-A(config-ve-2)# ip address 10.10.7.101 255.255.255.0
Zone1-SI-A(config-ve-2)# exit
```

The following command configures an IP default route. The next hop for this route is the ServerIron ADX's interface with firewall FW1.

```
Zone1-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
```

The following command configures a static route to the sub-net that contains the external host.

```
Zone1-SI-A(config)# ip route 20.20.0.0 255.255.0.0 10.10.7.100
```

The following commands configure the synchronization link between this ServerIron ADX and ServerIron ADX Zone1-SI-B. For redundancy, the link is configured on a trunk group.

```
Zone1-SI-A(config)# vlan 10
Zone1-SI-A(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone1-SI-A(config-vlan-10)# exit
Zone1-SI-A(config)# trunk switch ethernet 4/9 to 4/10
Zone1-SI-A(config)# trunk deploy
Zone1-SI-A(config)# server fw-port 4/9
```

The following commands configure the data link connecting this ServerIron ADX to its partner, Zone1-SI-B. For redundancy, the link is configured as a two-port trunk group.

```
Zone1-SI-A(config)# trunk switch ethernet 4/11 to 4/12
Zone1-SI-A(config)# trunk deploy
Zone1-SI-A(config)# server partner-ports ethernet 4/11
Zone1-SI-A(config)# server partner-ports ethernet 4/12
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# l2-fwall
Zone1-SI-A(config-fw-2)# exit
```

The following commands add the firewalls. Three application ports (HTTP, FTP, and SNMP) are configured on each of the firewalls. The **no-health-check** parameter disables the Layer 4 health check for the specified application.

```
Zone1-SI-A(config)# server fw-name fw1 10.10.1.1
Zone1-SI-A(config-rs-fw1)# port http
Zone1-SI-A(config-rs-fw1)# port http no-health-check
Zone1-SI-A(config-rs-fw1)# port snmp
Zone1-SI-A(config-rs-fw1)# port snmp no-health-check
Zone1-SI-A(config-rs-fw1)# exit
Zone1-SI-A(config)# server fw-name fw2 10.10.1.2
Zone1-SI-A(config-rs-fw2)# port http
Zone1-SI-A(config-rs-fw2)# port http no-health-check
Zone1-SI-A(config-rs-fw2)# port snmp
Zone1-SI-A(config-rs-fw2)# port snmp no-health-check
Zone1-SI-A(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group (always group 2).

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fw-name fw1
Zone1-SI-A(config-fw-2)# fw-name fw2
```

The following command enables the active-active mode. For details about configuring this command, refer to "Enabling the active-active mode" on page 48.

```
Zone1-SI-A(config-fw-2)# sym-priority 255
```

The following commands add the paths through the firewalls to the ServerIron ADXs in zones 2 and 3. In addition, static MAC entries are added for the firewall interfaces.

> **NOTE**
> The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
Zone1-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 2 4/11 10.10.2.222 10.10.1.2
Zone1-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 4 4/11 10.10.2.223 10.10.1.2
Zone1-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.3.111 10.10.1.1
Zone1-SI-A(config-fw-2)# fwall-info 6 4/11 10.10.3.111 10.10.1.2
Zone1-SI-A(config-fw-2)# exit
```

The following commands set the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. For example, the ServerIron ADX will load balance HTTP requests based on the firewall that has fewer HTTP session entries in the ServerIron ADX session table.

```
Zone1-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone1-SI-A(config-fw-2)# exit
```

The following commands configure standard IP ACLs for the IP sub-nets in one of the zones this ServerIron ADX is not in.

```
Zone1-SI-A(config)# access-list 2 permit 10.10.2.0 0.0.0.255
Zone1-SI-A(config)# access-list 2 permit 10.10.8.0 0.0.0.255
```

The following commands configure the zone parameters. To configure a zone, specify a name for the zone, and then a zone number (from 1 through 10), followed by the number of the ACL that specifies the IP addresses in the zone. In this example, the ACL numbers and zone numbers are the same, but this is not required.

```
Zone1-SI-A(config)# server fw-group 2
Zone1-SI-A(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-A(config-fw-2)# exit
```

The following commands configure the SLB information. Each of the servers in zones 2 and 3 is added as a real server, and then the servers are bound to a virtual IP. The servers are added using the **server remote-name** command instead of the **server real-name** command because the servers are not directly connected to the ServerIron ADX. Instead, they are connected to the ServerIron ADX through other routers (in this case, the firewalls).

```
Zone1-SI-A(config)# server remote-name web1 10.10.8.40
Zone1-SI-A(config-rs-web1)# port http
Zone1-SI-A(config-rs-web1)# exit
Zone1-SI-A(config)# server remote-name web2 10.10.8.42
Zone1-SI-A(config-rs-web2)# port http
Zone1-SI-A(config-rs-web2)# exit
Zone1-SI-A(config)# server remote-name web3 10.10.6.41
Zone1-SI-A(config-rs-web3)# port http
Zone1-SI-A(config-rs-web3)# exit
Zone1-SI-A(config)# server remote-name web4 10.10.6.43
Zone1-SI-A(config-rs-web4)# port http
Zone1-SI-A(config-rs-web4)# exit
Zone1-SI-A(config)# server virtual www.web.com 10.10.1.10
Zone1-SI-A(config-vs-www.web.com)# port http
```

```
Zone1-SI-A(config-vs-www.web.com)# bind http web1 http web2 http web3 http web4
http
Zone1-SI-A(config-vs-www.web.com)# exit
```

The following command enables SLB-to-FWLB.

```
Zone1-SI-A(config)# server slb-fw
```

The following command saves the configuration changes to the startup-config file.

```
Zone1-SI-A(config)# write memory
```

Commands on zone 1's standby ServerIron ADX (Zone1-SI-S)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone1-SI-S
Zone1-SI-S(config)# vlan 1
Zone1-SI-S(config-vlan-1)# always-active
Zone1-SI-S(config-vlan-1)# exit
Zone1-SI-S(config)# vlan 2
Zone1-SI-S(config-vlan-2)# always-active
Zone1-SI-S(config-vlan-2)# tagged ethernet 4/11 to 4/12
Zone1-SI-S(config-vlan-2)# untagged ethernet 4/1 to 4/8
Zone1-SI-S(config-vlan-2)# router-interface ve 1
Zone1-SI-S(config-vlan-2)# exit
Zone1-SI-S(config)# interface ve 1
Zone1-SI-S(config-ve-1)# ip address 10.10.1.112 255.255.255.0
Zone1-SI-S(config-ve-1)# exit
Zone1-SI-S(config)# vlan 20
Zone1-SI-S(config-vlan-20)# always-active
Zone1-SI-S(config-vlan-20)# tagged ethernet 4/11 to 4/12
Zone1-SI-S(config-vlan-20)# untagged ethernet 4/13 to 4/24
Zone1-SI-S(config-vlan-20)# router-interface ve 2
Zone1-SI-S(config-vlan-20# exit
Zone1-SI-S(config)# interface ve 2
Zone1-SI-S(config-ve-2)# ip address 10.10.7.102 255.255.255.0
Zone1-SI-S(config-ve-2)# exit
Zone1-SI-S(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.2
Zone1-SI-S(config)# ip route 20.20.0.0 255.255.0.0 10.10.7.100
Zone1-SI-S(config)# vlan 10
Zone1-SI-S(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone1-SI-S(config-vlan-10)# exit
Zone1-SI-S(config)# trunk switch ethernet 4/9 to 4/10
Zone1-SI-S(config)# trunk deploy
Zone1-SI-S(config)# server fw-port 4/9
Zone1-SI-S(config)# trunk switch ethernet 4/11 to 4/12
Zone1-SI-S(config)# trunk deploy
Zone1-SI-S(config)# server partner-ports ethernet 4/11
Zone1-SI-S(config)# server partner-ports ethernet 4/12
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# l2-fwall
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# server fw-name fw1 10.10.1.1
Zone1-SI-S(config-rs-fw1)# port http
Zone1-SI-S(config-rs-fw1)# port http no-health-check
Zone1-SI-S(config-rs-fw1)# port snmp
Zone1-SI-S(config-rs-fw1)# port snmp no-health-check
Zone1-SI-S(config-rs-fw1)# exit
Zone1-SI-S(config)# server fw-name fw2 10.10.1.2
```

```
Zone1-SI-S(config-rs-fw2)# port http
Zone1-SI-S(config-rs-fw2)# port http no-health-check
Zone1-SI-S(config-rs-fw2)# port snmp
Zone1-SI-S(config-rs-fw2)# port snmp no-health-check
Zone1-SI-S(config-rs-fw2)# exit
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# fw-name fw1
Zone1-SI-S(config-fw-2)# fw-name fw2
Zone1-SI-S(config-fw-2)# sym-priority 1
Zone1-SI-S(config-fw-2)# fwall-info 1 4/11 10.10.2.222 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 2 4/1 10.10.2.222 10.10.1.2
Zone1-SI-S(config-fw-2)# fwall-info 3 4/11 10.10.2.223 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 4 4/1 10.10.2.223 10.10.1.2
Zone1-SI-S(config-fw-2)# fwall-info 5 4/11 10.10.3.111 10.10.1.1
Zone1-SI-S(config-fw-2)# fwall-info 6 4/1 10.10.3.111 10.10.1.2
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config-fw-2)# fw-predictor per-service-least-conn
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# access-list 2 permit 10.10.2.0 0.0.0.255
Zone1-SI-S(config)# access-list 2 permit 10.10.8.0 0.0.0.255
Zone1-SI-S(config)# server fw-group 2
Zone1-SI-S(config-fw-2)# fwall-zone Zone2 2 2
Zone1-SI-S(config-fw-2)# exit
Zone1-SI-S(config)# server remote-name web1 10.10.8.40
Zone1-SI-S(config-rs-web1)# port http
Zone1-SI-S(config-rs-web1)# exit
Zone1-SI-S(config)# server remote-name web2 10.10.8.42
Zone1-SI-S(config-rs-web2)# port http
Zone1-SI-S(config-rs-web2)# exit
Zone1-SI-S(config)# server remote-name web3 10.10.6.41
Zone1-SI-S(config-rs-web3)# port http
Zone1-SI-S(config-rs-web3)# exit
Zone1-SI-S(config)# server remote-name web4 10.10.6.43
Zone1-SI-S(config-rs-web4)# port http
Zone1-SI-S(config-rs-web4)# exit
Zone1-SI-S(config)# server virtual www.web.com 10.10.1.10
Zone1-SI-S(config-vs-www.web.com)# port http
Zone1-SI-S(config-vs-www.web.com)# bind http web1 http web2 http web3 http web4
http
Zone1-SI-S(config-vs-www.web.com)# exit
Zone1-SI-S(config)# server slb-fw
Zone1-SI-S(config)# write memory
```

Commands on zone 2's active ServerIron ADX (Zone2-SI-A)

The following commands configure ServerIron ADX Zone2-SI-A in zone 2. The configuration is similar to the configuration for ServerIron ADX Zone1-SI-A, except the ACL and zone information are for zone 3, and FWLB-to-SLB is enabled instead of SLB-to-FWLB.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone2-SI-A
Zone2-SI-A(config)# vlan 1
Zone2-SI-A(config-vlan-1)# always-active
Zone1-SI-A(config)# vlan 2
Zone1-SI-A(config-vlan-2)# always-active
Zone1-SI-A(config-vlan-2)# tagged ethernet 4/11 to 4/12
Zone1-SI-A(config-vlan-2)# untagged ethernet 4/1 to 4/8
Zone1-SI-A(config-vlan-2)# router-interface ve 1
```

```
Zone1-SI-A(config-vlan-2)# exit
Zone1-SI-A(config)# interface ve 1
Zone1-SI-A(config-ve-1)# ip address 10.10.2.222 255.255.255.0
Zone1-SI-A(config-ve-1)# exit
Zone1-SI-A(config)# vlan 20
Zone1-SI-A(config-vlan-20)# always-active
Zone1-SI-A(config-vlan-20)# tagged ethernet 4/11 to 4/12
Zone1-SI-A(config-vlan-20)# untagged ethernet 4/13 to 4/24
Zone1-SI-A(config-vlan-20)# router-interface ve 2
Zone1-SI-A(config-vlan-20# exit
Zone1-SI-A(config)# interface ve 2
Zone1-SI-A(config-ve-2)# ip address 10.10.8.101 255.255.255.0
Zone1-SI-A(config-ve-2)# exit
Zone2-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.1
Zone2-SI-A(config)# vlan 10
Zone2-SI-A(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone2-SI-A(config-vlan-10)# exit
Zone2-SI-A(config)# trunk switch ethernet 4/9 to 4/10
Zone2-SI-A(config)# trunk deploy
Zone2-SI-A(config)# server fw-port 4/9
Zone2-SI-A(config)# trunk switch ethernet 4/11 to 4/12
Zone2-SI-A(config)# trunk deploy
Zone2-SI-A(config)# server partner-ports ethernet 4/11
Zone2-SI-A(config)# server partner-ports ethernet 4/12
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# l2-fwall
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# server fw-name fw1 10.10.2.1
Zone2-SI-A(config-rs-fw1)# port http
Zone2-SI-A(config-rs-fw1)# port http no-health-check
Zone2-SI-A(config-rs-fw1)# port ftp
Zone2-SI-A(config-rs-fw1)# port ftp no-health-check
Zone2-SI-A(config-rs-fw1)# port snmp
Zone2-SI-A(config-rs-fw1)# port snmp no-health-check
Zone2-SI-A(config-rs-fw1)# exit
Zone2-SI-A(config)# server fw-name fw2 10.10.2.2
Zone2-SI-A(config-rs-fw2)# port http
Zone2-SI-A(config-rs-fw2)# port http no-health-check
Zone2-SI-A(config-rs-fw2)# port ftp
Zone2-SI-A(config-rs-fw2)# port ftp no-health-check
Zone2-SI-A(config-rs-fw2)# port snmp
Zone2-SI-A(config-rs-fw2)# port snmp no-health-check
Zone2-SI-A(config-rs-fw2)# exit
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fw-name fw1
Zone2-SI-A(config-fw-2)# fw-name fw2
Zone2-SI-A(config-fw-2)# sym-priority 255
Zone2-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 2 4/11 10.10.1.111 10.10.2.2
Zone2-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 4 4/11 10.10.1.112 10.10.2.2
Zone2-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.3.111 10.10.2.1
Zone2-SI-A(config-fw-2)# fwall-info 6 4/11 10.10.3.111 10.10.2.2
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# access-list 3 permit 10.10.3.0 0.0.0.255
Zone2-SI-A(config)# access-list 3 permit 10.10.6.0 0.0.0.255
```

```
Zone2-SI-A(config)# server fw-group 2
Zone2-SI-A(config-fw-2)# fwall-zone zone3 3 3
Zone2-SI-A(config-fw-2)# exit
Zone2-SI-A(config)# server real-name rs1 10.10.8.40
Zone2-SI-A(config-rs-rs1)# port http
Zone2-SI-A(config-rs-rs1)# exit
Zone2-SI-A(config)# server real-name rs1 10.10.8.42
Zone2-SI-A(config-rs-rs2)# port http
Zone2-SI-A(config-rs-rs2)# exit
Zone2-SI-A(config)# server virtual www.rs.com 10.10.8.10
Zone2-SI-A(config-vs-www.rs.com)# port http
Zone2-SI-A(config-vs-www.web.com)# bind http rs1 http rs2 http
Zone2-SI-A(config-vs-www.web.com)# exit
Zone2-SI-A(config)# server fw-slb
Zone2-SI-A(config)# write memory
```

Commands on zone 2's standby ServerIron ADX (Zone2-SI-S)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone2-SI-S
Zone2-SI-S(config)# vlan 1
Zone2-SI-S(config-vlan-1)# always-active
Zone1-SI-S(config)# vlan 2
Zone1-SI-S(config-vlan-2)# always-active
Zone1-SI-S(config-vlan-2)# tagged ethernet 4/11 to 4/12
Zone1-SI-S(config-vlan-2)# untagged ethernet 4/1 to 4/8
Zone1-SI-S(config-vlan-2)# router-interface ve 1
Zone1-SI-S(config-vlan-2)# exit
Zone1-SI-S(config)# interface ve 1
Zone1-SI-S(config-ve-1)# ip address 10.10.2.223 255.255.255.0
Zone1-SI-S(config-ve-1)# exit
Zone1-SI-S(config)# vlan 20
Zone1-SI-S(config-vlan-20)# always-active
Zone1-SI-S(config-vlan-20)# tagged ethernet 4/11 to 4/12
Zone1-SI-S(config-vlan-20)# untagged ethernet 4/13 to 4/24
Zone1-SI-S(config-vlan-20)# router-interface ve 2
Zone1-SI-S(config-vlan-20# exit
Zone1-SI-S(config)# interface ve 2
Zone1-SI-S(config-ve-2)# ip address 10.10.8.102 255.255.255.0
Zone1-SI-S(config-ve-2)# exit
Zone2-SI-S(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.2
Zone2-SI-S(config)# vlan 10
Zone2-SI-S(config-vlan-10)# untagged ethernet 4/9 to 4/10
Zone2-SI-S(config-vlan-10)# exit
Zone2-SI-S(config)# trunk switch ethernet 4/9 to 4/10
Zone2-SI-S(config)# trunk deploy
Zone2-SI-S(config)# server fw-port 4/9
Zone2-SI-S(config)# trunk switch ethernet 4/11 to 4/12
Zone2-SI-S(config)# trunk deploy
Zone2-SI-S(config)# server partner-ports ethernet 4/11
Zone2-SI-S(config)# server partner-ports ethernet 4/12
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# l2-fwall
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# server fw-name fw1 10.10.2.1
Zone2-SI-S(config-rs-fw1)# port http
Zone2-SI-S(config-rs-fw1)# port http no-health-check
Zone2-SI-S(config-rs-fw1)# port ftp
```

```
Zone2-SI-S(config-rs-fw1)# port ftp no-health-check
Zone2-SI-S(config-rs-fw1)# port snmp
Zone2-SI-S(config-rs-fw1)# port snmp no-health-check
Zone2-SI-S(config-rs-fw1)# exit
Zone2-SI-S(config)# server fw-name fw2 10.10.2.2
Zone2-SI-S(config-rs-fw2)# port http
Zone2-SI-S(config-rs-fw2)# port http no-health-check
Zone2-SI-S(config-rs-fw2)# port ftp
Zone2-SI-S(config-rs-fw2)# port ftp no-health-check
Zone2-SI-S(config-rs-fw2)# port snmp
Zone2-SI-S(config-rs-fw2)# port snmp no-health-check
Zone2-SI-S(config-rs-fw2)# exit
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fw-name fw1
Zone2-SI-S(config-fw-2)# fw-name fw2
Zone2-SI-S(config-fw-2)# sym-priority 1
Zone2-SI-S(config-fw-2)# fwall-info 1 4/11 10.10.1.111 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 2 4/1 10.10.1.111 10.10.2.2
Zone2-SI-S(config-fw-2)# fwall-info 3 4/11 10.10.1.112 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 4 4/1 10.10.1.112 10.10.2.2
Zone2-SI-S(config-fw-2)# fwall-info 5 4/11 10.10.3.111 10.10.2.1
Zone2-SI-S(config-fw-2)# fwall-info 6 4/1 10.10.3.111 10.10.2.2
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fw-predictor per-service-least-conn
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# access-list 3 permit 10.10.3.0 0.0.0.255
Zone2-SI-S(config)# access-list 3 permit 10.10.6.0 0.0.0.255
Zone2-SI-S(config)# server fw-group 2
Zone2-SI-S(config-fw-2)# fwall-zone zone3 3 3
Zone2-SI-S(config-fw-2)# exit
Zone2-SI-S(config)# server real-name rs1 10.10.8.40
Zone2-SI-S(config-rs-rs1)# port http
Zone2-SI-S(config-rs-rs1)# exit
Zone2-SI-S(config)# server real-name rs1 10.10.8.42
Zone2-SI-S(config-rs-rs2)# port http
Zone2-SI-S(config-rs-rs2)# exit
Zone2-SI-S(config)# server virtual www.rs.com 10.10.8.10
Zone2-SI-S(config-vs-www.rs.com)# port http
Zone2-SI-S(config-vs-www.web.com)# bind http rs1 http rs2 http
Zone2-SI-S(config-vs-www.web.com)# exit
Zone2-SI-S(config)# server fw-slb
Zone2-SI-S(config)# write memory
```

Commands on zone 3's ServerIron ADX (Zone3-SI-A)

The following commands configure the ServerIron ADX in zone 3.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname Zone3-SI-A
Zone3-SI-A(config)# vlan 1
Zone3-SI-A(config-vlan-1)# untagged ethernet 4/1 to 4/12
Zone3-SI-A(config-vlan-1)# router-interface ve 1
Zone3-SI-A(config-vlan-1)# exit
Zone3-SI-A(config)# interface ve 1
Zone3-SI-A(config-ve-1)# ip address 10.10.3.111 255.255.255.0
Zone3-SI-A(config-ve-1)# exit
```

```
Zone3-SI-A(config)# vlan 2
Zone3-SI-A(config-vlan-2)# untagged ethernet 4/13 to 4/24
Zone3-SI-A(config-vlan-2)# router-interface ve 2
Zone3-SI-A(config-vlan-2)# exit
Zone3-SI-A(config)# interface ve 2
Zone3-SI-A(config-ve-1)# ip address 10.10.6.101 255.255.255.0
Zone3-SI-A(config-ve-1)# exit
Zone3-SI-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.3.1
Zone3-SI-A(config)# server fw-name fw1 10.10.3.1
Zone3-SI-A(config-rs-fw1)# port http
Zone3-SI-A(config-rs-fw1)# port http no-health-check
Zone3-SI-A(config-rs-fw1)# port ftp
Zone3-SI-A(config-rs-fw1)# port ftp no-health-check
Zone3-SI-A(config-rs-fw1)# port snmp
Zone3-SI-A(config-rs-fw1)# port snmp no-health-check
Zone3-SI-A(config-rs-fw1)# exit
Zone3-SI-A(config)# server fw-name fw2 10.10.3.2
Zone3-SI-A(config-rs-fw2)# port http
Zone3-SI-A(config-rs-fw2)# port http no-health-check
Zone3-SI-A(config-rs-fw2)# port ftp
Zone3-SI-A(config-rs-fw2)# port ftp no-health-check
Zone3-SI-A(config-rs-fw2)# port snmp
Zone3-SI-A(config-rs-fw2)# port snmp no-health-check
Zone3-SI-A(config-rs-fw2)# exit
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fw-name fw1
Zone3-SI-A(config-fw-2)# fw-name fw2
Zone3-SI-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 2 4/2 10.10.1.111 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 4 4/2 10.10.1.112 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 5 4/1 10.10.2.222 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 6 4/2 10.10.2.222 10.10.3.2
Zone3-SI-A(config-fw-2)# fwall-info 7 4/1 10.10.2.223 10.10.3.1
Zone3-SI-A(config-fw-2)# fwall-info 8 4/2 10.10.2.223 10.10.3.2
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fw-predictor per-service-least-conn
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# access-list 2 permit 10.10.2.0 0.0.0.255
Zone3-SI-A(config)# access-list 2 permit 10.10.8.0 0.0.0.255
Zone3-SI-A(config)# server fw-group 2
Zone3-SI-A(config-fw-2)# fwall-zone zone2 2 2
Zone3-SI-A(config-fw-2)# exit
Zone3-SI-A(config)# server real-name sr1 10.10.6.41
Zone3-SI-A(config-rs-sr1)# port http
Zone3-SI-A(config-rs-sr1)# exit
Zone3-SI-A(config)# server real-name sr2 10.10.6.43
Zone3-SI-A(config-rs-sr2)# port http
Zone3-SI-A(config-rs-sr2)# exit
Zone3-SI-A(config)# server virtual www.sr.com 10.10.6.10
Zone3-SI-A(config-vs-www.rs.com)# port http
Zone3-SI-A(config-vs-www.web.com)# bind http sr2 http sr1 http
Zone3-SI-A(config-vs-www.web.com)# exit
Zone3-SI-A(config)# server fw-slb
Zone3-SI-A(config)# write memory
```

Configuring FWLB for NAT Firewalls

In this chapter

NAT firewalls

Some Layer 3 firewalls perform Network Address Translation (NAT). These firewalls translate private addresses on the private side of the network into public (Internet) addresses on the public side of the network.

NOTE
The configuration steps for firewalls that perform NAT are identical to the steps for basic and IronClad FWLB without NAT, with just one additional step. The additional step disables load balancing for the NAT addresses.

You can deploy ServerIron ADXs to load balance NAT firewalls in a basic configuration or an IronClad configuration, just as in the examples in the previous chapters. Configuring the ServerIron ADXs for NAT requires only one additional step. The additional step disables load balancing for the NAT addresses, which are the addresses the firewalls use when translating private addresses into Internet addresses.

You can configure a single ServerIron ADX on each side of the firewalls (as in the basic configuration example in Figure 18) or you can configure active-standby pairs of ServerIron ADXs on each side of the firewalls (as in Figure 19).

Firewalls perform NAT in a couple of ways. The ServerIron ADX supports load balancing for either method and the ServerIron ADX configuration is the same for each method. You do not need to know which method your firewalls are using to configure the ServerIron ADXs to load balance for them.

The methods to perform NAT are as follows:

• Hiding internal addresses behind a single public address – The firewall is configured with a single Internet address that it uses for clients that initiate traffic from within the private side of the network. The firewall translates the source address for such traffic from the private address of the client into the public address. The firewall keeps track of the private addresses by including a Layer 4 port number from a pool of such numbers. When the firewall receives a return packet from a destination, the firewall uses the port number to identify the correct private address and translates the packet's destination address from the public address into the correct private address.

- Static translation – For traffic from a client inside the private network to a destination on the Internet, the firewall translates the private address into a unique Internet address. Likewise, for traffic from the Internet, the firewall translates the public address into a private address. Unlike the previous method, the static method assigns a different, unique Internet address for each client in the private network. The previous method uses a common Internet address for all private addresses.

Configuring basic Layer 3 FWLB for NAT firewalls

Figure 18 shows an example of a basic FWLB configuration for Layer 3 NAT firewalls. The procedures and CLI configuration example in this section are based on this sample configuration.

NOTE
The configuration steps for firewalls that perform NAT are identical to the steps for basic and IronClad FWLB without NAT, with just one additional step. The additional step disables load balancing for the NAT addresses. Refer to "Preventing load balancing of the NAT addresses" on page 118.

FIGURE 18   FWLB for Layer 3 firewalls performing NAT—basic configuration
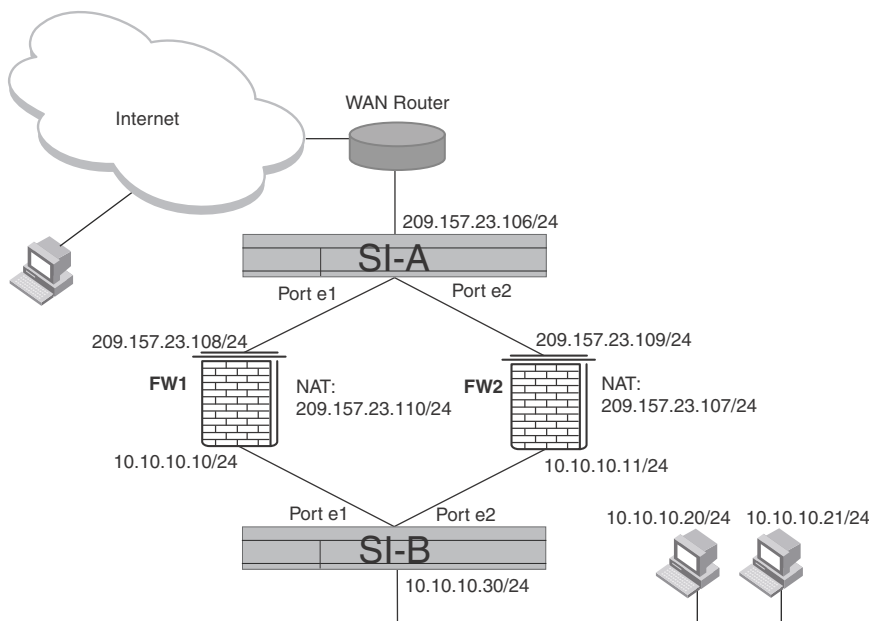
To configure basic Layer 3 FWLB for NAT firewalls, perform the tasks shown in Table 6.

TABLE 6   Basic FWLB for NAT firewalls configuration tasks

Task	Reference
Configure global parameters	
Configure firewall parameters	
Define the firewalls and add them to the firewall group	page 115

TABLE 6   Basic FWLB for NAT firewalls configuration tasks (Continued)

Task	Reference
Configure firewall group parameters	
Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX	page 116
Configure NAT address parameters	
Disable load balancing for the NAT addresses	page 118

Defining the firewalls and adding them to the firewall group

When FWLB is enabled, all the ServerIron ADX ports are in firewall group 2 by default. However, you must add an entry for each firewall, and then add the firewalls to the firewall group. To add an entry for a firewall, specify the firewall name and IP address. You can specify a name up to 32 characters long.

NOTE
When static NAT is used on firewalls in FWLB configurations, the ServerIron ADX virtual routing interface IP addresses that are in firewalls subnets should be excluded from NAT translation to prevent the firewall paths from failing health checks.

To define the firewalls (shown in Figure 18) using the CLI, enter the following commands.

Commands for ServerIron ADX A (external)

```
ServerIronADX-A(config)# server fw-name fw1 209.157.23.108
ServerIronADX-A(config-rs-fw1)# exit
ServerIronADX-A(config)# server fw-name fw2 209.157.23.109
ServerIronADX-A(config-rs-fw2)# exit
ServerIronADX-A(config)# server fw-group 2
ServerIronADX-A(config-fw-2)# fw-name fw1
ServerIronADX-A(config-fw-2)# fw-name fw2
```

Commands for ServerIron ADX B (internal)

```
ServerIronADX-B(config)# server fw-name fw1 10.10.10.10
ServerIronADX-B(config-rs-fw1)# exit
ServerIronADX-B(config)# server fw-name fw2 10.10.10.11
ServerIronADX-B(config-rs-fw2)# exit
ServerIronADX-B(config)# server fw-group 2
ServerIronADX-B(config-fw-2)# fw-name fw1
ServerIronADX-B(config-fw-2)# fw-name fw2
```

Syntax: [no] server fw-name *<string> <ip-addr>|<ipv6-addr>*

NOTE
When you add a firewall name, the CLI level changes to the firewall level. This level is used when you configure stateful FWLB.

Syntax: server fw-group 2 | 4

This command changes the CLI to the firewall group configuration level. The IPv4 address format firewall group number is 2. The IPv6 address format firewall group number is 4. These are the only supported firewall groups.

Syntax: [no] fw-name *<string>*

This command adds a configured firewall to the firewall group.

Configuring the paths and adding static MAC entries

A path is configuration information the ServerIron ADX uses to ensure that a given source and destination IP pair is always authenticated by the same Layer 3 firewall.

Each path consists of the following parameters:

- The path ID – A number that identifies the path. The paths go from one ServerIron ADX to the other through the firewalls.

- The ServerIron ADX port – The number of the port that connects the ServerIron ADX to the firewall.

- The other ServerIron ADX's or Layer 2 switch's IP address – The management address of the ServerIron ADX or Layer 2 switch on the other side of the firewall. The ServerIron ADX on the private network side and the other ServerIron ADX or Layer 2 switch are the endpoints of the data path through the firewall.

- The next-hop IP address – The IP address of the firewall interface connected to this ServerIron ADX.

For each type of firewall (Layer 3 synchronous and asynchronous, with or without NAT), you must configure paths between the ServerIron ADXs through the firewalls.

In addition to configuring the paths, you must create a static MAC entry for each firewall interface attached to the ServerIron ADX.

> **NOTE**
> FWLB paths must be fully meshed. When you configure a FWLB path on a ServerIron ADX, make sure you also configure a reciprocal path on the ServerIron ADX attached to the other end of the firewalls. For example, if you configure four paths to four separate firewalls, make sure you configure four paths on the other ServerIron ADX.

> **NOTE**
> The static MAC entries are required. You must add a static MAC entry for each firewall interface with the ServerIron ADX.

To configure the paths and static MAC entries for the configuration shown in Figure 2 on page 11, enter the following commands. Enter the first group of commands on ServerIron ADX A. Enter the second group of commands on ServerIron ADX B.

Commands for ServerIron ADX A (external)

```
ServerIronADX-A(config)# server fw-group 2
ServerIronADX-A(config-fw-2)# fwall-info 1 1 10.10.10.30 209.157.23.108
ServerIronADX-A(config-fw-2)# fwall-info 2 2 10.10.10.30 209.157.23.109
ServerIronADX-A(config-fw-2)# exit
```

```
ServerIronADX-A(config)# static-mac-address abcd.da10.dc2c ethernet 1 priority 1
router-type
ServerIronADX-A(config)# static-mac-address abcd.da10.dc3f ethernet 2 priority 1
router-type
```

Commands for ServerIron ADX B (internal)

```
ServerIronADX-B(config)# server fw-group 2
ServerIronADX-B(config-fw-2)# fwall-info 1 1 209.157.23.106 10.10.10.10
ServerIronADX-B(config-fw-2)# fwall-info 2 2 209.157.23.106 10.10.10.11
ServerIronADX-B(config-fw-2)# exit
ServerIronADX-B(config)# static-mac-address abcd.da68.6655 ethernet 1 priority 1
router-type
ServerIronADX-B(config)# static-mac-address abcd.da68.6104 ethernet 2 priority 1
router-type
```

Syntax: server fw-group 2 | 4

This command changes the CLI to the firewall group configuration level. The IPv4 address format firewall group number is 2. The IPv6 address format firewall group number is 4. These are the only supported firewall groups.

Syntax: (IPv4) [no] fwall-info *<path-num>* *<portnum>* *<other-ip>* *<next-hop-ip>*

Syntax: (IPv6) [no] fwall-info *<path-num>* *<portnum>* *<other-ipv6>* *<next-hop-ipv6>*

NOTE
The other IP address and next-hop IP address parameters must be both IPv4 addresses or both IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

NOTE
You must use IPv4 addresses for IPv4 firewalls and IPv6 addresses for IPv6 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

The *<path-num>* parameter specifies the path. The sequence of path IDs must be contiguous from start to finish.

The *<portnum>* parameter specifies the port that connects the ServerIron ADX to the firewall. If the port number is dynamic, use port number 65535.

The *<other-ip>* parameter specifies the IPv4 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ip>* parameter specifies the IPv4 address of the firewall connected to this ServerIron ADX.

The *<other-ipv6>* parameter specifies the IPv6 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ipv6>* parameter specifies the IPv6 address of the firewall connected to this ServerIron ADX.

Syntax: [no] static-mac-address *<mac-addr>* **ethernet** *<portnum>* [priority *<0-7>*] [host-type |
router-type]

The priority can be from 0 through 7 (0 is lowest and 7 is highest). The defaults are **host-type** and **0**.

NOTE
The static MAC entries are required. You must add a static MAC entry for each firewall interface with
the ServerIron ADX. In addition, you must use the **priority 1** and **router-type** parameters with the
static-mac-address command. These parameters enable the ServerIron ADX to use the address for
FWLB.

NOTE
If you enter the **static-mac-address** command at the global CONFIG level, the static MAC entry
applies to the default port-based VLAN (VLAN 1). If you enter the **static-mac-address** command at
the configuration level for a specific port-based VLAN, the entry applies to that VLAN and not to the
default VLAN.

Preventing load balancing of the NAT addresses

When you configure ServerIron ADXs for load balancing traffic across NAT firewalls, you must
disable load balancing on the NAT addresses themselves.   You can use either of the following
methods to do so. Each method is equally valid and only one of the methods is required. You need
to use one of these methods only on the ServerIron ADX connected to the external network, not the
ServerIron ADX on the internal side of the network.

The methods for preventing load balancing of the NAT addresses are as follows:

- Configure the NAT addresses as firewall addresses, but do not configure paths for the
  addresses. (This is shown in the "Extra Firewall Method" section.)

- Configure IP access policies (filters) to deny load balancing for traffic addressed to the NAT
  addresses. (This is shown in the "Access Policy Method" section.)

NOTE
In FWLB configurations, the IP policies do not block traffic altogether. They deny load balancing
for the traffic. Thus, the ServerIron ADX does not load balance packets addressed to the NAT
addresses, but instead sends the traffic only to the firewall that originally sent the traffic.

Extra firewall method

To disable load balancing for the NAT addresses by adding firewalls for the addresses, enter
commands such as the following.

NOTE
Do not configure paths for the firewalls.

```
ServerIronADX-A(config)# server fw-name fw3NAT 209.157.23.107
ServerIronADX-A(config-rs-fw3NAT)# exit
ServerIronADX-A(config)# server fw-name fw4NAT 209.157.23.110
ServerIronADX-A(config-rs-fw4NAT)# exit
```

Access policy method

To disable load balancing for the NAT addresses using IP access policies, enter commands such as the following.

```
ServerIronADX-A(config)# ip filter 1 deny any 209.157.23.110 255.255.255.255
ServerIronADX-A(config)# ip filter 2 deny any 209.157.23.107 255.255.255.255
ServerIronADX-A(config)# ip filter 1024 permit any any
```

The first two commands configure policies to deny load balancing for the two NAT addresses. The third command allows all other traffic to be load balanced.

NOTE
The third policy, which permits all traffic, is required because once you define an access policy, the default action for packets that do not match a policy is to deny them. Thus, if you configure only the first two policies and not the third one, you actually disable load balancing altogether by denying the load balancing for all packets.

Configuration example for FWLB with Layer 3 NAT firewalls

This section shows the CLI commands for implementing the configuration shown in Figure 18. Note that the configuration steps are similar to those required for the basic configuration shown in Figure 2 on page 11. The only additional step required is to ensure that the ServerIronADX connected to the external network does not load balance return traffic to the addresses the firewalls use for NAT. For example, ServerIron ADX A in Figure 18 must be configured so that it does not load balance return traffic to 209.157.23.107/24 or 209.157.23.110/24.

CLI commands on ServerIron ADX A (external)

The following commands configure ServerIronADX-A in Figure 18 for FWLB.

The **hostname** command changes the host name of the device to match the name used in Figure 18. The **ip address** and **ip default-gateway** commands configure the device's management IP address and its default gateway.

The **no span** command disables the Spanning Tree Protocol (STP) on the ServerIronADX.

```
ServerIronADX(config)# hostname ServerIronADX-A
ServerIronADX-A(config)# ip address 209.157.23.106 255.255.255.0
ServerIronADX-A(config)# ip default-gateway 209.157.23.108
ServerIronADX-A(config)# no span
```

The following commands add the firewalls. The IP addresses are the firewalls' interfaces with the ServerIron ADX.

```
ServerIronADX-A(config)# server fw-name fw1 209.157.23.108
ServerIronADX-A(config-rs-fw1)# exit
ServerIronADX-A(config)# server fw-name fw2 209.157.23.109
ServerIronADX-A(config-rs-fw2)# exit
```

The following commands add firewall entries for the hidden NAT addresses. These entries prevent the ServerIron ADX from load balancing the firewall traffic to these addresses. The ServerIron ADX forwards a return packet addressed to one of these firewalls directly to the firewall that sent it, instead of using the hash mechanism to select a path for the traffic.

```
ServerIronADX-A(config)# server fw-name fw3NAT 209.157.23.107
ServerIronADX-A(config-rs-fw3NAT)# exit
ServerIronADX-A(config)# server fw-name fw4NAT 209.157.23.110
ServerIronADX-A(config-rs-fw4NAT)# exit
```

The following commands configure the firewall group parameters. The first commands change the CLI to the firewall group configuration level. The **fw-name** commands add the firewalls. Notice that the firewall definitions created previously for the two NAT addresses are not added.

The **fw-name** *<firewall-name>* command adds the firewalls to the firewall group.

The **fwall-info** commands add paths from this ServerIron ADX to the other one through the firewalls. Notice that no paths are configured for the firewall definitions created for the NAT addresses.

```
ServerIronADX-A(config)# server fw-group 2
ServerIronADX-A(config-fw-2)# fw-name fw1
ServerIronADX-A(config-fw-2)# fw-name fw2
ServerIronADX-A(config-fw-2)# fwall-info 1 1 10.10.10.30 209.157.23.108
ServerIronADX-A(config-fw-2)# fwall-info 2 2 10.10.10.30 209.157.23.109
ServerIronADX-A(config-fw-2)# exit
```

The following commands add static MAC entries for the firewalls' interfaces with the ServerIron ADX. The **priority 1** and **router-type** parameters are required for FWLB with Layer 3 firewalls.

```
ServerIronADX-A(config)# static-mac-address abcd.da10.dc2c ethernet 1 priority 1
router-type
ServerIronADX-A(config)# static-mac-address abcd.da10.dc3f ethernet 2 priority 1
router-type
```

The **write memory** command saves the configuration changes to the ServerIron ADX's startup-config file on the device's flash memory.

```
ServerIronADX-A(config)# write memory
```

Alternative configuration for ServerIron ADX A

The previous example configures FWLB for NAT firewalls by adding firewall definitions for the IP addresses the NAT service on the firewalls uses for traffic sent from a client inside the firewalls to a destination outside the firewalls.

Alternatively, you can configure IP access policies that deny load balancing for the NAT addresses. For the example in , you would enter the following commands.

```
ServerIronADX-A(config)# ip filter 1 deny any 209.157.23.110 255.255.255.255
ServerIronADX-A(config)# ip filter 2 deny any 209.157.23.107 255.255.255.255
ServerIronADX-A(config)# ip filter 1024 permit any any
```

The first two commands configure policies to deny load balancing for the two NAT addresses. The third command allows all other traffic to be load balanced.

NOTE
The third policy, which permits all traffic, is required because once you define an access policy, the default action for packets that do not match a policy is to deny them. Thus, if you configure only the first two policies and not the third one, you actually disable load balancing altogether by denying the load balancing for all packets.

The other commands are the same as in the previous section.

CLI commands on ServerIron ADX B (internal)

The following CLI commands configure ServerIron ADX B in Figure 18. Notice that this ServerIron ADX is not configured to deny load balancing for the NAT addresses used by the firewalls. This ServerIron ADX sees only the internal addresses, not the NAT addresses.

```
ServerIronADX-B(config)# hostname ServerIronADX-B
ServerIronADX-B(config)# ip address 10.10.10.30 255.255.255.0
ServerIronADX-B(config)# ip default-gateway 10.10.10.10
ServerIronADX-B(config)# no span
ServerIronADX-B(config)# server fw-name fw1 10.10.10.10
ServerIronADX-B(config-rs-fw1)# exit
ServerIronADX-B(config)# server fw-name fw2 10.10.10.11
ServerIronADX-B(config-rs-fw2)# exit
ServerIronADX-B(config)# server fw-group 2
ServerIronADX-B(config-fw-2)# fw-name fw1
ServerIronADX-B(config-fw-2)# fw-name fw2
ServerIronADX-B(config-fw-2)# fwall-info 1 1 209.157.23.106 10.10.10.10
ServerIronADX-B(config-fw-2)# fwall-info 2 2 209.157.23.106 10.10.10.11
ServerIronADX-B(config-fw-2)# exit
ServerIronADX-B(config)# static-mac-address abcd.da68.6655 ethernet 1 priority 1
router-type
ServerIronADX-B(config)# static-mac-address abcd.da68.6104 ethernet 2 priority 1
router-type
```

Configuring IronClad Layer 3 FWLB for NAT

Figure 19 shows an example of an IronClad FWLB configuration for Layer 3 NAT firewalls. The procedures and CLI configuration example in this section are based on this sample configuration.

NOTE
The configuration steps for firewalls that perform NAT are identical to the steps for basic and IronClad FWLB without NAT, with just one additional step. The additional step disables load balancing for the NAT addresses. Refer to "Preventing load balancing of the NAT addresses" on page 128.

FIGURE 19   FWLB for Layer 3 firewalls performing NAT—IronClad configuration
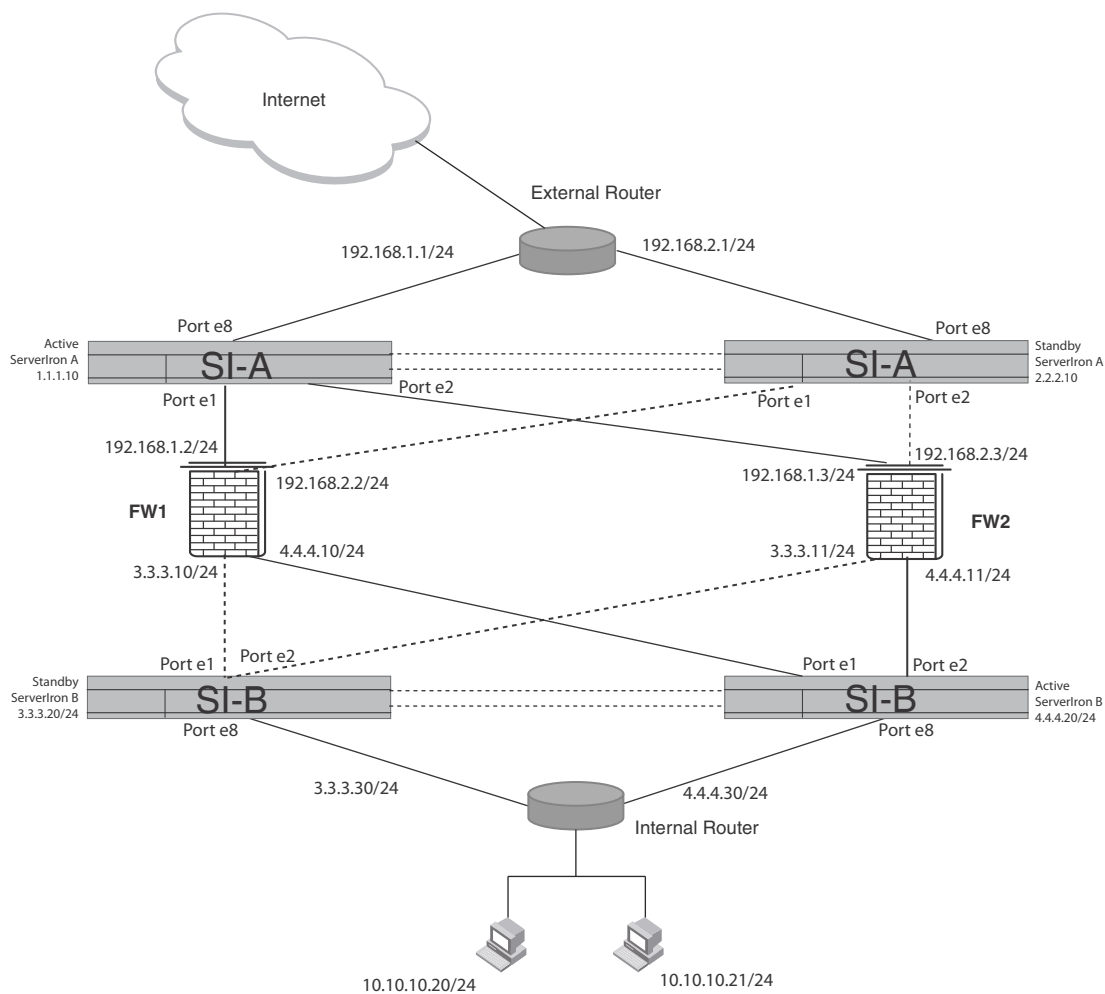
To configure IronClad FWLB for NAT firewalls, perform the tasks shown in Figure 7 on page 122.

TABLE 7   IronClad FWLB for NAT firewalls configuration tasks

Task	Reference
Configure global parameters	
Identify the partner port (the link between the active and standby ServerIron ADXs)	page 123
Identify the router port (ServerIron ADX ports connected to routers)	page 123
Configure firewall parameters	
Define the firewalls and add them to the firewall group	page 123
Configure firewall group parameters	
Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX	page 125
Specify the ServerIron ADX priority (determines which ServerIron ADX in the active-standby pair is the default active ServerIron ADX)	page 128

TABLE 7   IronClad FWLB for NAT firewalls configuration tasks (Continued)

Task	Reference
Configure NAT address parameters	
Disable load balancing for the NAT addresses	page 128

Specifying the partner port

If you are configuring the ServerIron ADX for IronClad FWLB, you need to specify the port number of the dedicated link between the ServerIron ADX and its partner.

To specify the port, enter a command such as the following at the global CLI level.

```
ServerIronADX(config)# server fw-port 5
```

Syntax: [no] server fw-port <*portnum*>

If the link between the two ServerIron ADXs is a trunk group (recommended for added redundancy), specify the port number of the primary port. The primary port is the first port in the trunk group.

Specifying the router ports

IronClad FWLB configurations require paths to the routers as part of the active-standby configuration for the ServerIron ADXs. You must identify the ports on the ServerIron ADX that are attached to the routers.

To identify port 8 on a ServerIron ADX as a router port, enter the following command.

```
ServerIronADX(config)# server router-port 8
```

Syntax: [no] server router-port <*portnum*>

NOTE
To define multiple router ports on a switch, enter the port numbers separated by blanks. You can enter up to eight router ports in a single command line. To enter more than eight ports, enter the **server router-port** command again with the additional ports.

Defining the firewalls and adding them to the firewall group

When FWLB is enabled, all the ServerIron ADX ports are in firewall group 2 by default. However, you must add an entry for each firewall. To add an entry for a firewall, specify the firewall name and IP address. You can specify a name up to 32 characters long. After you add the firewall entries, add the firewalls to the firewall group.

To define the firewalls shown in Figure 19 on page 122, use the following method.

Commands for active ServerIron ADX A (external active)

```
SI-ActiveA(config)# server fw-name fw1 192.168.1.2
SI-ActiveA(config-rs-fw1)# exit
SI-ActiveA(config)# server fw-name fw2 192.168.1.3
SI-ActiveA(config-rs-fw2)# exit
SI-ActiveA(config)# server fw-group 2
SI-ActiveA(config-fw-2)# fw-name fw1
SI-ActiveA(config-fw-2)# fw-name fw2
```

Commands for standby ServerIron ADX A (external standby)

```
SI-StandbyA(config)# server fw-name fw1 192.168.2.2
SI-StandbyA(config-rs-fw1)# exit
SI-StandbyA(config)# server fw-name fw2 192.168.2.3
SI-StandbyA(config-rs-fw2)# exit
SI-StandbyA(config)# fw-group 2
SI-StandbyA(config-fw-2)# fw-name fw1
SI-StandbyA(config-fw-2)# fw-name fw2
```

Commands for active ServerIron ADX B (internal active)

```
SI-ActiveB(config)# server fw-name fw1 4.4.4.10
SI-ActiveB(config-rs-fw1)# exit
SI-ActiveB(config)# server fw-name fw2 4.4.4.11
SI-ActiveB(config-rs-fw2)# exit
SI-ActiveB(config)# server fw-group 2
SI-ActiveB(config-fw-2)# fw-name fw1
SI-ActiveB(config-fw-2)# fw-name fw2
```

Commands for standby ServerIron ADX B (internal standby)

```
SI-StandbyB(config)# server fw-name fw1 3.3.3.10
SI-StandbyB(config-rs-fw1)# exit
SI-StandbyB(config)# server fw-name fw2 3.3.3.11
SI-StandbyB(config-rs-fw2)# exit
SI-StandbyB(config)# server fw-group 2
SI-StandbyB(config-fw-2)# fw-name fw1
SI-StandbyB(config-fw-2)# fw-name fw2
```

Syntax: **[no] server fw-name** *<string> <ip-addr>|<ipv6-addr>*

NOTE

When you add a firewall name, the CLI level changes to the firewall level. This level is used when you configure stateful FWLB.

Syntax: **server fw-group 2 | 4**

This command changes the CLI to the firewall group configuration level. The IPv4 address format firewall group number is 2. The IPv6 address format firewall group number is 4. These are the only supported firewall groups.

Syntax: **[no] fw-name** *<string>*

This command adds a configured firewall to the firewall group.

Configuring paths and adding static MAC entries for Layer 3 firewalls

A path is configuration information the ServerIron ADX uses to ensure that a given source and destination IP pair is always authenticated by the same Layer 3 firewall.

Each path consists of the following parameters:

- The path ID – A number that identifies the path. In basic FWLB configurations, the paths go from one ServerIron ADX to the other through the firewalls. The paths go from one ServerIron ADX to the ServerIron ADXs in the other active-standby pair other through the firewalls. A path also goes to the router.

- The ServerIron ADX port – The number of the port that connects the ServerIron ADX to the firewall.

- The other ServerIron ADX's or Layer 2 switch's IP address – The management address of the ServerIron ADX or Layer 2 switch on the other side of the firewall. The ServerIron ADX on the private network side and the other ServerIron ADX or Layer 2 switch are the endpoints of the data path through the firewall.

- The next-hop IP address – The IP address of the firewall interface connected to this ServerIron ADX.

For each type of firewall (Layer 3 synchronous and asynchronous, with or without NAT), you must configure paths between the ServerIron ADXs through the firewalls.

In addition to configuring the paths, you must create a static MAC entry for each firewall interface attached to the ServerIron ADX.

NOTE
FWLB paths must be fully meshed. When you configure a FWLB path on a ServerIron ADX, make sure you also configure a reciprocal path on the ServerIron ADX attached to the other end of the firewalls. For example, if you configure four paths to four separate firewalls, make sure you configure four paths on the other ServerIron ADX.

NOTE
The static MAC entries are required. You must add a static MAC entry for each firewall interface with the ServerIron ADX.

To configure the paths and static MAC entries for the configuration shown in Figure 19 on page 122, enter the following commands. Enter the first group of commands on ServerIron ADX A. Enter the second group of commands on ServerIron ADX B.

Commands for active ServerIron ADX A (external active)

```
SI-ActiveA(config)# server fw-group 2
SI-ActiveA(config-fw-2)# fwall-info 1 1 3.3.3.20 192.168.1.2
SI-ActiveA(config-fw-2)# fwall-info 2 2 3.3.3.20 192.168.1.3
SI-ActiveA(config-fw-2)# fwall-info 3 1 4.4.4.20 192.168.1.2
SI-ActiveA(config-fw-2)# fwall-info 4 2 4.4.4.20 192.168.1.3
SI-ActiveA(config-fw-2)# fwall-info 5 8 192.168.1.1 192.168.1.1
SI-ActiveA(config-fw-2)# exit
SI-ActiveA(config)# static-mac-address abcd.4321.2498 ethernet 1 priority 1
router-type
SI-ActiveA(config)# static-mac-address abcd.4321.a53c ethernet 2 priority 1
router-type
```

Commands for standby ServerIron ADX A (external standby)

```
SI-StandbyA(config)# server fw-group 2
SI-StandbyA(config-fw-2)# fwall-info 1 1 3.3.3.20 192.168.2.2
SI-StandbyA(config-fw-2)# fwall-info 2 2 3.3.3.20 192.168.2.3
SI-StandbyA(config-fw-2)# fwall-info 3 1 4.4.4.20 192.168.2.2
SI-StandbyA(config-fw-2)# fwall-info 4 2 4.4.4.20 192.168.2.3
SI-StandbyA(config-fw-2)# fwall-info 5 8 192.168.2.1 192.168.2.1
SI-StandbyA(config-fw-2)# exit
SI-StandbyA(config)# static-mac-address abcd.4321.a53d ethernet 2 priority 1
router-type
SI-StandbyA(config)# static-mac-address abcd.4321.2499 ethernet 1 priority 1
router-type
```

Commands for active ServerIron ADX B (internal active)

```
SI-ActiveB(config)# server fw-group 2
SI-ActiveB(config-fw-2)# fwall-info 1 1 192.168.2.10 4.4.4.10
SI-ActiveB(config-fw-2)# fwall-info 2 2 192.168.2.10 4.4.4.11
SI-ActiveB(config-fw-2)# fwall-info 3 1 192.168.1.10 4.4.4.10
SI-ActiveB(config-fw-2)# fwall-info 4 2 192.168.1.10 4.4.4.11
SI-ActiveB(config-fw-2)# fwall-info 5 8 4.4.4.30 4.4.4.30
SI-ActiveB(config-fw-2)# exit
SI-ActiveB(config)# static-mac-address abcd.4321.249b ethernet 1 high-priority
router-type
SI-ActiveB(config)# static-mac-address abcd.4321.a53f ethernet 2 high-priority
router-type
```

Commands for standby ServerIron ADX B (internal standby)

```
SI-StandbyB(config)# server fw-group 2
SI-StandbyB(config-fw-2)# fwall-info 1 1 192.168.1.10 3.3.3.10
SI-StandbyB(config-fw-2)# fwall-info 2 2 192.168.1.10 3.3.3.11
SI-StandbyB(config-fw-2)# fwall-info 3 1 192.168.2.10 3.3.3.10
SI-StandbyB(config-fw-2)# fwall-info 4 2 192.168.2.10 3.3.3.11
SI-StandbyB(config-fw-2)# fwall-info 5 8 3.3.3.30 3.3.3.30
SI-StandbyB(config-fw-2)# exit
SI-StandbyB(config)# static-mac-address abcd.4321.a53e ethernet 2 priority 1
router-type
SI-StandbyB(config)# static-mac-address abcd.4321.249a ethernet 1 priority 1
router-type
```

Syntax: server fw-group 2 | 4

This command changes the CLI to the firewall group configuration level. The IPv4 address format firewall group number is 2. The IPv6 address format firewall group number is 4. These are the only supported firewall groups.

Syntax: (IPv4) [no] fwall-info *<path-num> <portnum> <other-ip> <next-hop-ip>*

Syntax: (IPv6) [no] fwall-info *<path-num> <portnum> <other-ipv6> <next-hop-ipv6>*

NOTE
The other IP address and next-hop IP address parameters must be both IPv4 addresses or both IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

NOTE
You must use IPv4 addresses for IPv4 firewalls and IPv6 addresses for IPv6 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

The *<path-num>* parameter specifies the path. The sequence of path IDs must be contiguous from start to finish.

The *<portnum>* parameter specifies the port that connects the ServerIron ADX to the firewall. If the port number is dynamic, use port number 65535.

The *<other-ip>* parameter specifies the IPv4 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ip>* parameter specifies the IPv4 address of the firewall connected to this ServerIron ADX.

The *<other-ipv6>* parameter specifies the IPv6 address of the ServerIron ADX on the other side of the firewall.

The *<next-hop-ipv6>* parameter specifies the IPv6 address of the firewall connected to this ServerIron ADX.

Syntax: [no] static-mac-address *<mac-addr>* ethernet *<portnum>* [priority *<0-7>*] [host-type | router-type]

The priority can be from 0 through 7 (0 is lowest and 7 is highest). The defaults are **host-type** and **0.**

NOTE
The static MAC entries are required. You must add a static MAC entry for each firewall interface with the ServerIron ADX. In addition, you must use the **priority 1** and **router-type** parameters with the **static-mac-address** command. These parameters enable the ServerIron ADX to use the address for FWLB.

NOTE
If you enter the **static-mac-address** command at the global CONFIG level, the static MAC entry applies to the default port-based VLAN (VLAN 1). If you enter the **static-mac-address** command at the configuration level for a specific port-based VLAN, the entry applies to that VLAN and not to the default VLAN.

Configuring the ServerIron ADX priority

If you are configuring the ServerIron ADX for IronClad FWLB, you must specify the priority for the firewalls within the firewall group. The priority determines which of the partner ServerIron ADXs that are configured together for IronClad FWLB is the default active ServerIron ADX for the firewalls within the group.

You can specify a priority from 0 through 255.   The ServerIron ADX with the higher priority is the default active ServerIron ADX for the firewalls within the firewall group.

NOTE
If you specify 0, the CLI removes the priority. When you save the configuration to the startup-config file, the **sym-priority** command is removed. You cannot remove the priority using the **no sym-priority** command.

To configure a ServerIron ADX to be the default active ServerIron ADX for the firewalls in group 2, enter the following commands.

Commands for active ServerIron ADX A (external active)

```
SI-ActiveA(config)# server fw-group 2
SI-ActiveA(config-fw-2)# sym-priority 255
```

Commands for standby ServerIron ADX A (external standby)

To configure another ServerIron ADX to not be the default active ServerIron ADX for the firewalls in group 2, enter the following commands.

```
SI-StandbyA(config)# server fw-group 2
SI-StandbyA(config-fw-2)# sym-priority 1
```

Commands for active ServerIron ADX B (internal active)

```
SI-ActiveB(config)# server fw-group 2
SI-ActiveB(config-fw-2)# sym-priority 255
```

Commands for standby ServerIron ADX B (internal standby)

```
SI-StandbyB(config)# server fw-group 2
SI-StandbyB(config-fw-2)# sym-priority 1
```

Syntax: [no] sym-priority *<num>*

The *<num>* variable can be from 0 through 255.

Preventing load balancing of the NAT addresses

To prevent load balancing of the NAT address when configuring an IronClad FWLB for Layer 3 NAT firewalls, refer to

Configuration example for IronClad FWLB with Layer 3 NAT firewalls

This section shows the CLI commands for implementing the configuration shown in Figure 19 on page 122. The only additional step required is to ensure that the ServerIron ADX connected to the external network does not load balance return traffic to the addresses the firewalls use for NAT. For example, ServerIron ADX A in Figure 19 on page 122 must be configured so that it does not load balance return traffic to 192.168.2.10/24 or 192.168.2.3/24.

To prevent the ServerIron ADX from load balancing the NAT addresses, you can use either of the following methods. Each method is equally valid and only one of the methods is required. You need to use one of these methods only on the ServerIron ADX connected to the external network, not the ServerIron ADX on the internal side of the network. Consider the following methods:

- Configure the NAT addresses as firewall addresses, but do not configure paths for the addresses.
- Configure IP access policies (filters) to deny load balancing for traffic addressed to the NAT addresses.

NOTE
In FWLB configurations, the IP policies do not block traffic altogether. They deny load balancing for the traffic. Thus, the ServerIron ADX does not load balance packets addressed to the NAT addresses, but instead sends the traffic only to the firewall that originally sent the traffic.

Commands on active ServerIron ADX A (external active)

The following commands add a management IP address and default gateway address to the ServerIron ADX. For the configuration in this example, the ServerIron ADX needs to be in only one sub-net, so additional IP addresses are not added. However, the IP address must be in the same sub-net as the ServerIron ADX's interface to the Layer 3 firewalls.

```
SI-ActiveA(config)# ip address 192.168.1.10/24
SI-ActiveA(config)# ip default-gateway 192.168.1.2
```

The following commands configure the ports for the connection to the standby ServerIron ADX in a separate port-based VLAN. This is required.

```
SI-ActiveA(config)# vlan 10 by port
SI-ActiveA(config-vlan-10)# untagged 5 to 6
SI-ActiveA(config-vlan-10)# exit
```

The **trunk** command creates a trunk group for the ports that connect this ServerIron ADX to its partner. Using a trunk group for the link between the active and standby ServerIron ADXs is not required, but using a trunk group adds an additional level of redundancy for enhanced availability. If one of the ports in a trunk group goes down, the link remains intact as long as the other port remains up. Since the trunk group is between two ServerIron ADX switches, make sure you configure a switch trunk group, not a server trunk group.

```
SI-ActiveA(config)# trunk switch ethernet 5 to 6
SI-ActiveA(config)# trunk deploy
```

The **server router-port** command identifies the port that connects this ServerIron ADX to the router connected to the other ServerIron ADX in the active-standby pair.

```
SI-ActiveA(config)# server router-port 8
```

The **server fw-port** command identifies the port that connects this ServerIron ADX to its partner. If you configure a trunk group for the link between the two partners, specify the first port (the primary port for the group) in the trunk group.

```
SI-ActiveA(config)# server fw-port 5
```

The **server fw-name** commands add the firewalls to the ServerIron ADX. In the commands above, "fw1" and "fw2" are the firewall names. These names are specific to the ServerIron ADX and do not need to correspond to any name parameters on the firewalls themselves. The IP addresses are the addresses of the firewall interfaces with the ServerIron ADX.

```
SI-ActiveA(config)# server fw-name fw1 192.168.1.2
SI-ActiveA(config-rs-fw1)# exit
SI-ActiveA(config)# server fw-name fw2 192.168.1.3
SI-ActiveA(config-rs-fw2)# exit
```

The following commands add firewall entries for the hidden NAT addresses. These entries prevent the ServerIron ADX from load balancing the firewall traffic to these addresses. The ServerIron ADX forwards a return packet addressed to one of these firewalls directly to the firewall that sent it, instead of using the hash mechanism to select a path for the traffic.

```
ServerIronADX-A(config)# server fw-name fw3NAT 192.168.2.10
ServerIronADX-A(config-rs-fw3NAT)# exit
ServerIronADX-A(config)# server fw-name fw4NAT 192.168.2.3
ServerIronADX-A(config-rs-fw4NAT)# exit
```

The following commands configure the firewall group. The **server fw-group 2** command changes the focus of the CLI to firewall group 2 (IPv4 addresses). The **server fw-group 4** command changes the focus of the CLI to firewall group 4 (IPv6 addresses).

The **sym-priority** command specifies the priority of this ServerIron ADX with respect to the other ServerIron ADX for the firewalls in the firewall group. The priority can be from 0 through 255. The ServerIron ADX with the higher priority is the default active ServerIron ADX for the firewalls within the group.

NOTE
If you specify 0, the CLI removes the priority. When you save the configuration to the startup-config file, the **sym-priority** command is removed. Use this method to remove the priority. You cannot remove the priority using the **no sym-priority** command.

The **fw-name** *<firewall-name>* command adds the firewalls to the firewall group. Notice that the firewall entries for the hidden NAT addresses are not added.

```
SI-ActiveA(config)# server fw-group 2
SI-ActiveA(config-fw-2)# sym-priority 255
SI-ActiveA(config-fw-2)# fw-name fw1
SI-ActiveA(config-fw-2)# fw-name fw2
```

The **fwall-info** commands add the paths between this ServerIron ADX and the other ServerIron ADXs through the firewalls. The paths enhance performance by ensuring that a given traffic flow (source and destination IP addresses) always travels through the same firewall. In configurations that use asynchronous firewalls, the paths enhance performance by eliminating excess authentications. In this configuration, each ServerIron ADX has two paths to each of the two firewalls. The fifth path goes to the router.

The paths are required, even if the firewalls are synchronized.

The first parameter with each command is a path ID. The second parameter is the port number of the ServerIron ADX port that connects the ServerIron ADX to the firewall in the path.

The third parameter is the IP address of the ServerIron ADX at the other end of the path or, for paths to routers, the IP address of the router's interface with the ServerIron ADX. Note that each ServerIron ADX has a path to each of the ServerIron ADXs in the other pair, but does not have a path to its own standby pair.

The fourth parameter is the IP address of the firewall or router interface with this ServerIron ADX. Notice that the ServerIron ADX has two paths for each firewall. One of the paths goes to the active ServerIron ADX in the other pair. The other path goes to the standby ServerIron ADX in the pair. In the case of the path to the router, the third and fourth parameters have the same value.

```
SI-ActiveA(config-fw-2)# fwall-info 1 1 3.3.3.20 192.168.1.2
SI-ActiveA(config-fw-2)# fwall-info 2 2 3.3.3.20 192.168.1.3
SI-ActiveA(config-fw-2)# fwall-info 3 1 4.4.4.20 192.168.1.2
SI-ActiveA(config-fw-2)# fwall-info 4 2 4.4.4.20 192.168.1.3
SI-ActiveA(config-fw-2)# fwall-info 5 8 192.168.1.1 192.168.1.1
SI-ActiveA(config-fw-2)# exit
```

The following commands add static entries to the ServerIron ADX's MAC table for the firewall interfaces. The priority 1 and router-type parameters are required for FWLB.

```
SI-ActiveA(config)# vlan 1
SI-ActiveA(config-vlan-1)# static-mac-address abcd.4321.2498 ethernet 1 priority
1 router-type
SI-ActiveA(config-vlan-1)# static-mac-address abcd.4321.a53c ethernet 2 priority
1 router-type
SI-ActiveA(config-vlan-1)# exit
```

NOTE
If you enter the command at the global CONFIG level, the static MAC entry applies to the default port-based VLAN (VLAN 1). If you enter the command at the configuration level for a specific port-based VLAN, the entry applies to that VLAN and not to the default VLAN.

Alternative configuration for active ServerIron ADX A

The previous example configures FWLB for NAT firewalls by adding firewall definitions for the IP addresses the NAT service on the firewalls uses for traffic sent from a client inside the firewalls to a destination outside the firewalls.

Alternatively, you can configure IP access policies that deny load balancing for the NAT addresses. For the example in Figure 19 on page 122, you would enter the following commands.

```
ServerIronADX-A(config)# ip filter 1 deny any 192.168.2.3 255.255.255.255
ServerIronADX-A(config)# ip filter 2 deny any 192.168.3.2 255.255.255.255
ServerIronADX-A(config)# ip filter 1024 permit any any
```

The first two commands configure policies to deny load balancing for the two NAT addresses. The third command allows all other traffic to be load balanced.

NOTE
The third policy, which permits all traffic, is required because once you define an access policy, the default action for packets that do not match a policy is to deny them. Thus, if you configure only the first two policies and not the third one, you actually disable load balancing altogether by denying the load balancing for all packets.

The other commands are the same as in the previous section.

Commands on standby ServerIron ADX A (external standby)

```
SI-StandbyA(config)# ip address 192.168.2.10/24
SI-StandbyA(config)# ip default-gateway 192.168.2.2
SI-StandbyA(config)# vlan 10 by port
SI-StandbyA(config-vlan-10)# untagged 5 to 6
SI-StandbyA(config-vlan-10)# exit
SI-StandbyA(config)# trunk switch ethernet 5 to 6
SI-StandbyA(config)# trunk deploy
SI-StandbyA(config)# server router-port 8
SI-StandbyA(config)# server fw-port 5
SI-StandbyA(config)# server fw-name fw2-1 192.168.2.2
SI-StandbyA(config-rs-fw2-1)# exit
SI-StandbyA(config)# server fw-name fw2-2 192.168.2.3
SI-StandbyA(config-rs-fw2-2)# exit
SI-StandbyA(config)# server fw-group 2
SI-StandbyA(config-fw-2)# sym-priority 1
SI-StandbyA(config-fw-2)# fw-name fw1
SI-StandbyA(config-fw-2)# fw-name fw2
SI-StandbyA(config-fw-2)# fwall-info 1 1 3.3.3.20 192.168.2.2
SI-StandbyA(config-fw-2)# fwall-info 2 2 3.3.3.20 192.168.2.3
SI-StandbyA(config-fw-2)# fwall-info 3 1 4.4.4.20 192.168.2.2
SI-StandbyA(config-fw-2)# fwall-info 4 2 4.4.4.20 192.168.2.3
SI-StandbyA(config-fw-2)# fwall-info 5 8 192.168.2.1 192.168.2.1
SI-StandbyA(config-fw-2)# exit
SI-StandbyA(config)# vlan 1
SI-StandbyA(config-vlan-1)# static-mac-address abcd.4321.a53d ethernet 2 priority
1 router-type
SI-StandbyA(config-vlan-1)# static-mac-address abcd.4321.2499 ethernet 1 priority
1 router-type
SI-StandbyA(config-vlan-1)# exit
SI-StandbyA(config)# write memory
```

Alternative configuration for standby ServerIron ADX A

The previous example configures FWLB for NAT firewalls by adding firewall definitions for the IP addresses the NAT service on the firewalls uses for traffic sent from a client inside the firewalls to a destination outside the firewalls.

Alternatively, you can configure IP access policies that deny load balancing for the NAT addresses. For the example in Figure 19 on page 122, you would enter the following commands.

```
SI-StandbyA(config)# ip filter 1 deny any 192.168.2.3 255.255.255.255
SI-StandbyA(config)# ip filter 2 deny any 192.168.3.2 255.255.255.255
SI-StandbyA(config)# ip filter 1024 permit any any
```

The first two commands configure policies to deny load balancing for the two NAT addresses. The third command allows all other traffic to be load balanced.

NOTE
The third policy, which permits all traffic, is required because once you define an access policy, the default action for packets that do not match a policy is to deny themfire wallshus, if you configure only the first two policies and not the third one, you actually disable load balancing altogether by denying the load balancing for all packets.

The other commands are the same as in the previous section.

Commands on active ServerIron ADX B (internal active)

```
SI-ActiveB(config)# ip address 3.3.3.20/24
SI-ActiveB(config)# ip default-gateway 4.4.4.11
SI-ActiveB(config)# vlan 10 by port
SI-ActiveB(config-vlan-10)# untagged 5 to 6
SI-ActiveB(config-vlan-10)# exit
SI-ActiveB(config)# trunk switch ethernet 5 to 6
SI-ActiveB(config)# trunk deploy
SI-ActiveB(config)# server router-port 8
SI-ActiveB(config)# server fw-port 5
SI-ActiveB(config)# server fw-name fw2-1 4.4.4.10
SI-ActiveB(config-rs-fw2-1)# exit
SI-ActiveB(config)# server fw-name fw2-2 4.4.4.11
SI-ActiveB(config-rs-fw2-2)# exit
SI-ActiveB(config)# server fw-group 2
SI-ActiveB(config-fw-2)# sym-priority 255
SI-ActiveB(config-fw-2)# fw-name fw2-1
SI-ActiveB(config-fw-2)# fw-name fw2-2
SI-ActiveB(config-fw-2)# fwall-info 1 1 192.168.2.10 4.4.4.10
SI-ActiveB(config-fw-2)# fwall-info 2 2 192.168.2.10 4.4.4.11
SI-ActiveB(config-fw-2)# fwall-info 3 1 192.168.1.10 4.4.4.10
SI-ActiveB(config-fw-2)# fwall-info 4 2 192.168.1.10 4.4.4.11
SI-ActiveB(config-fw-2)# fwall-info 5 8 4.4.4.30 4.4.4.30
SI-ActiveB(config-fw-2)# exit
SI-ActiveB(config)# vlan 1
SI-ActiveB(config-vlan-1)# static-mac-address abcd.4321.249b ethernet 1 priority
1 router-type
SI-ActiveB(config-vlan-1)# static-mac-address abcd.4321.a53f ethernet 2 priority
1 router-type
SI-ActiveB(config-vlan-1)# exit
SI-ActiveB(config)# write memory
```

Configuring FWLB and SLB

In this chapter

FWLB and SLB configuration overview

NOTE
This chapter shows basic FWLB configurations with Layer 3 firewalls. Currently, these are the configurations supported by the ServerIron. If you need to perform concurrent SLB and FWLB in a different type of FWLB configuration, contact Brocade.

You can configure the ServerIron ADX to concurrently perform FWLB and SLB at the same time. The software supports the following configurations:

- SLB-to-FWLB – The ServerIron ADX on the Internet side of the firewalls performs FWLB for traffic directed toward real servers connected to the ServerIron ADX on the private side of the firewalls. In this configuration, all the SLB configuration (virtual IP address, real server, and port bindings) resides on the Internet ServerIron ADX. The real servers are configured as remote servers. In addition, the SLB-to-FWLB feature is enabled on the Internet ServerIron ADX. The internal ServerIron ADX is configured for FWLB but requires no additional configuration.

- FWLB-to-SLB – The internal ServerIron ADX (the one on the private side of the firewalls) contains all the SLB configuration information. In this configuration, the FWLB-to-SLB feature is enabled on this ServerIron ADX rather than the Internet ServerIron ADX. This configuration enables the internal ServerIron ADX to learn the firewall from which a client request is received and send the server reply back through the same firewall.

Your choice of implementation depends on the ServerIron ADX you want to use for the SLB configuration. Use SLB-to-FWLB if you want to place the SLB configuration on the Internet ServerIron ADX. Use FWLB-to-SLB is you want to place the SLB configuration on the internal ServerIron ADX.

NOTE
In FWLB HA configurations, sym-priority should not be configured under the virtual servers when both FWLB and SLB are configured. In FWLB HA configurations, the ServerIron ADX ADX that is active for the firewall group is also the owner of the virtual servers configured.

Figure 20 shows an example of an SLB-to-FWLB configuration.

FIGURE 20   SLB-to-FWLB configuration
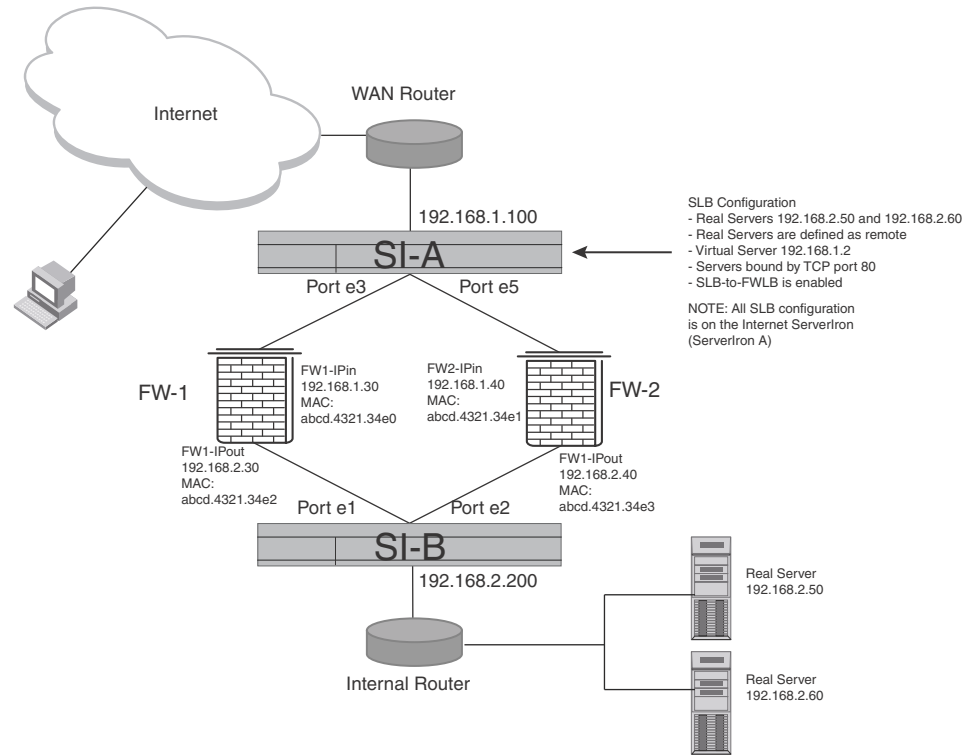
Notice that all the SLB configuration is on the Internet ServerIron ADX (ServerIron A).

Figure 21 shows an example of an FWLB-to-SLB configuration.

FIGURE 21   FWLB-to-SLB configuration
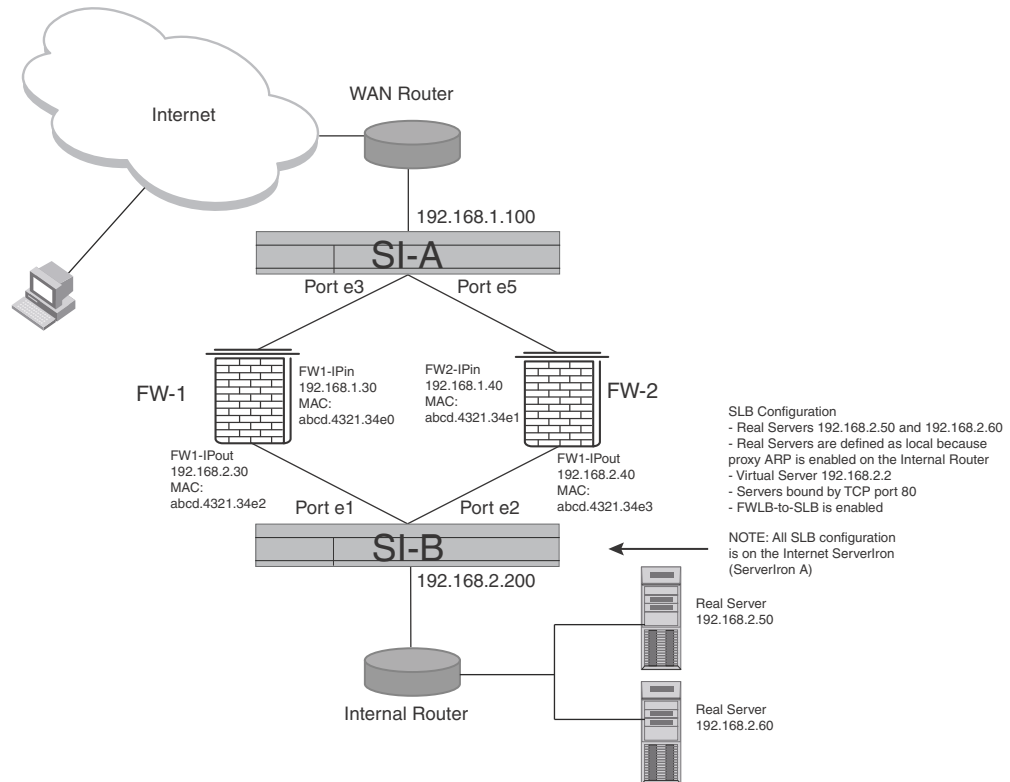
For FWLB-to-SLB, all the SLB configuration information is on the internal ServerIron ADX (ServerIron ADX B).

Configuring SLB-to-FWLB

To configure SLB-to-FWLB in a basic FWLB configuration for Layer 3 firewalls, such as the one shown in Figure 20, perform the following tasks:

- Configure SLB parameters on the Internet ServerIron:
  - Configure the real servers
  - Configure the virtual server
  - Bind the real servers to the virtual server
  - Enable the SLB-to-FWLB feature
- Configure global FWLB parameters
- Configure firewall parameters:

  Define the firewalls and add them to the firewall group

- Configure firewall group parameters:

  Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron ADX

The tasks under the first item (Configure SLB parameters on the Internet ServerIron ADX) are described in the following sections. The remaining tasks are identical to the tasks for configuring basic FWLB for Layer 3 firewalls. For more information about these tasks, refer to "Configuring basic Layer 3 FWLB" on page 17.

Configuring the SLB parameters

In an SLB-to-FWLB configuration, all SLB configuration takes place on the Internet ServerIron ADX. The ServerIron ADX on the private side of the firewalls does not contain any SLB configuration information. This section describes how to configure the Internet ServerIron ADX to provide SLB for the real servers and virtual server shown in Figure 20 on page 136.

Configuring the real servers

To configure the real servers shown in Figure 20 on page 136, enter the following commands on the Internet ServerIron ADX (ServerIron A).

NOTE
In SLB-to-FWLB configurations, you must define the real servers as remote servers.

```
ServerIronADXA(config)# server remote-name RS1 192.168.2.50
ServerIronADXA(config-rs-RS1)# port http
ServerIronADXA(config-rs-RS1)# exit
ServerIronADXA(config)# server remote-name RS2 192.168.2.60
ServerIronADXA(config-rs-RS2)# port http
ServerIronADXA(config-rs-RS2)# exit
```

The **server remote-name** command adds a real server. The port command enables a TCP or UDP port on the server. In this case, the **port http** command enables TCP port 80 (HTTP).

NOTE
If you use the **server real-name** command instead of the **server remote-name** command, the real servers are added as local servers. You must add them as remote servers for SLB-to-FWLB.

Syntax: [no] **server remote-name** *<text> <ip-addr>*

Syntax: [no] **port** *<port>* [disable | enable]

Syntax: [no] **port** *<port>* [keepalive]

Configuring the virtual server

To configure the virtual server shown in Figure 20 on page 136, enter the following command on the Internet ServerIron ADX (ServerIron A).

```
ServerIronADXA(config)# server virtual-name www.brocade.com 192.168.1.2
ServerIronADXA(config-vs-www.brocade.com)# port http
```

The **server virtual-name** command adds the virtual server. The **port** command enables a TCP or UDP port on the server.

Syntax: [no] **server virtual-name** *<text>* [*<ip-addr>*]

Binding the real server to the virtual server

To bind the real servers to the virtual server, enter the following commands on the Internet ServerIron ADX (ServerIron ADX A). Notice that the port binding takes place on the Virtual Server configuration level.

```
ServerIronADXA(config)# server virtual www.brocade.com
ServerIronADXA(config-vs-www.brocade.com)# bind http RS1 http
ServerIronADXA(config-vs-www.brocade.com)# bind http RS2 http
ServerIronADXA(config-vs-www.brocade.com)# exit
```

Syntax: [no] bind *<port> <real server name> <port>*

Enabling SLB-to-FWLB

To enable SLB-to-FWLB, enter the following command on the Internet ServerIron ADX (ServerIron ADX A).

```
ServerIronADXA(config)# server slb-fw
```

Syntax: [no] server slb-fw

Configuration example for SLB-to-FWLB

The following sections show all the ServerIron ADX commands you would enter on each ServerIron ADX to implement the SLB-to-FWLB configuration shown in Figure 20 on page 136.

Commands on ServerIron A (external)

Enter the following commands to configure SLB. In an SLB-to-FWLB configuration, all SLB configuration takes place on the Internet ServerIron ADX (ServerIron ADX A, the External ServerIron ADX, in this example).

The following commands change the ServerIron's host name to "ServerIronA", configure the ServerIron ADX's management IP address, and specify the default gateway.

```
ServerIronADX(config)# hostname ServerIronA
ServerIronADXA(config)# ip address 192.168.1.100 255.255.255.0
ServerIronADXA(config)# ip default-gateway 192.168.1.1
```

The following commands configure the real servers. Notice that the servers are configured as remote servers. This is required for SLB-to-FWLB.

```
ServerIronADXA(config)# server remote-name RS1 192.168.2.50
ServerIronADXA(config-rs-RS1)# port http
ServerIronADXA(config-rs-RS1)# exit
ServerIronADXA(config)# server remote-name RS2 192.168.2.60
ServerIronADXA(config-rs-RS2)# port http
ServerIronADXA(config-rs-RS2)# exit
```

The following commands configure the virtual server and bind it to the real servers with TCP port 80 (HTTP).

```
ServerIronADXA(config)# server virtual-name www.brocade.com 192.168.1.2
ServerIronADXA(config-vs-www.brocade.com)# port http
ServerIronADXA(config)# server virtual www.brocade.com
ServerIronADXA(config-vs-www.brocade.com)# bind http RS1 http
ServerIronADXA(config-vs-www.brocade.com)# bind http RS2 http
```

Enter the following command to enable SLB-to-FWLB.

NOTE
This command applies only to the ServerIron ADX that contains the SLB configuration. Do not enter this command on the internal ServerIron ADX (ServerIronB).

```
ServerIronADXA(config)# server slb-fw
```

The following commands add two firewalls, FW1-IPin and FW2-IPin.

```
ServerIronADXA(config)# server fw-name FW1-IPin 192.168.1.30
ServerIronADXA(config-rs-FW1-IPin)# exit
ServerIronADXA(config)# server fw-name FW2-IPin 192.168.1.40
ServerIronADXA(config-rs-FW2-IPin)# exit
```

The following commands configure parameters for firewall group 2. The **fwall-info** commands configure the paths for the firewall traffic. Each path consists of a path ID, the ServerIron port attached to the firewall, the IP address of the ServerIron ADX at the other end of the path, and the next-hop IP address (usually the firewall interface connected to this ServerIron). Make sure you configure reciprocal paths on the other ServerIron ADX, as shown in the section containing the CLI commands for ServerIron B.

NOTE
Path information is required even if the firewalls are synchronized.

The **fw-name** *<firewall-name>* command adds the firewalls to the firewall group.

```
ServerIronADXA(config)# server fw-group 2
ServerIronADXA(config-fw-2)# fw-name FW1-IPin
ServerIronADXA(config-fw-2)# fw-name FW2-IPin
ServerIronADXA(config-fw-2)# fwall-info 1 3 192.168.2.200 192.168.1.30
ServerIronADXA(config-fw-2)# fwall-info 2 5 192.168.2.200 192.168.1.40
ServerIronADXA(config-fw-2)# exit
```

The following commands add static MAC entries for the MAC addresses of the firewall interfaces connected to the ServerIron. Notice that the QoS priority is configured as **priority 1** and the **router-type** parameter is specified. These parameters are required.

NOTE
To ensure proper operation, always configure the path IDs so that the IDs consistently range from lowest path ID to highest path ID for the firewalls. For example, in Figure 20 on page 136, the path IDs should range from lowest to highest beginning with the firewall interface at the upper left of the figure.
To ensure smooth operation, you might want to depict your firewalls in a vertical hierarchy as in Figure 20 on page 136, label the interfaces with their IP addresses, then configure the paths so that the path IDs to the interfaces range from lowest to highest path ID starting from the uppermost firewall interface.

```
ServerIronADXA(config)# static-mac-address abcd.4321.34e0 ethernet 3 priority 1
router-type
ServerIronADXA(config)# static-mac-address abcd.4321.34e1 ethernet 5 priority 1
router-type
ServerIronADXA(config)# write memory
```

Commands on ServerIron B (internal)

Enter the following commands to configure FWLB on ServerIron B. Notice that the **fwall-info** commands configure paths that are reciprocal to the paths configured on ServerIron A. Path 1 on each ServerIron goes through one of the firewalls while path 2 goes through the other firewall.

```
ServerIronADXB(config)# server fw-name FW1-IPout 192.168.2.30
ServerIronADXB(config-rs-FW1-IPout)# exit
ServerIronADXB(config)# server fw-name FW2-IPout 192.168.2.40
ServerIronADXB(config-rs-FW2-IPout)# exit
ServerIronADXB(config)# server fw-group 2
ServerIronADXB(config-fw-2)# fw-name FW1-IPout
ServerIronADXB(config-fw-2)# fw-name FW2-IPout
ServerIronADXB(config-fw-2)# fwall-info 1 1 192.168.1.100 192.168.2.30
ServerIronADXB(config-fw-2)# fwall-info 2 2 192.168.1.100 192.168.2.40
ServerIronADXB(config-fw-2)# exit
ServerIronADXB(config)# static-mac-address abcd.4321.34e2 ethernet 1 priority 1
router-type
ServerIronADXB(config)# static-mac-address abcd.4321.34e3 ethernet 2 priority 1
router-type
ServerIronADXB(config)# write memory
```

Configuring FWLB-to-SLB

Configuration for FWLB-to-SLB is similar to configuration for SLB-to-FWLB, with the following differences:

- SLB configuration information resides on the internal ServerIron ADX, not on the Internet ServerIron ADX.

- The FWLB-to-SLB feature is enabled on the internal ServerIron ADX.

- If Proxy ARP is enabled on the internal router, you can define the real servers as local servers instead of remote servers. However, if Proxy ARP is not enabled on the internal router, the real servers must be remote servers.

To configure FWLB-to-SLB in a basic FWLB configuration for Layer 3 firewalls, such as the one shown in , perform the following tasks:

- Configure SLB parameters on the internal ServerIron:
    - Configure the real servers
    - Configure the virtual server
    - Bind the real servers to the virtual server
    - Enable the FWLB-to-SLB feature
- Configure global FWLB parameters

- Configure firewall parameters:

  Define the firewalls and add them to the firewall group

- Configure firewall group parameters:

  Configure the paths and add static MAC entries for the firewall interfaces with the ServerIron

The tasks under the first item (Configure SLB parameters on the internal ServerIron) are described in the following sections. The remaining tasks are identical to the tasks for configuring basic FWLB for Layer 3 firewalls. For more information about these tasks, refer to "Configuring basic Layer 3 FWLB" on page 17.

Configuring the SLB parameters

In an FWLB-to-SLB configuration, all SLB configuration takes place on the internal ServerIron ADX. The ServerIron ADX on the Internet side of the firewalls does not contain any SLB configuration information. This section describes how to configure the internal ServerIron ADX to provide SLB for the real servers and virtual server shown in Figure 21 on page 137.

Configuring the real servers

To configure the real servers shown in Figure 21 on page 137, enter the following commands on the internal ServerIron ADX (ServerIron ADX B).

NOTE
You can use the **server real-name** command if Proxy ARP is enabled on the internal router. Otherwise, you must use the **server remote-name** command to add the real servers instead of the **server real-name** command.

```
ServerIronADXB(config)# server real-name RS1 192.168.2.50
ServerIronADXB(config-rs-RS1)# port http
ServerIronADXB(config-rs-RS1)# exit
ServerIronADXB(config)# server real-name RS2 192.168.2.60
ServerIronADXB(config-rs-RS2)# port http
ServerIronADXB(config-rs-RS2)# exit
```

The **server real-name** command adds a real server. The port command enables a TCP or UDP port on the server. In this case, the **port http** command enables TCP port 80 (HTTP).

Syntax: [no] **server real-name** <*text*> <*ip-addr*>

Syntax: [no] **port** <*port*> [**disable | enable**]

Syntax: [no] **port** <*port*> [**keepalive**]

Configuring the virtual server

To configure the virtual server shown in Figure 21 on page 137, enter the following command on the internal ServerIron ADX (ServerIron B).

```
ServerIronADXB(config)# server virtual-name www.brocade.com 192.168.1.2
ServerIronADXB(config-vs-www.brocade.com)# port http
```

The **server virtual-name** command adds the virtual server. The **port** command enables a TCP or UDP port on the server.

Syntax: [no] **server virtual-name** <*text*> [<*ip-addr*>]

Binding the real server to the virtual server

To bind the real servers to the virtual server, enter the following commands on the internal ServerIron ADX (ServerIron ADX B). Notice that the port binding takes place on the Virtual Server configuration level.

```
ServerIronADXB(config)# server virtual www.brocade.com
ServerIronADXB(config-vs-www.brocade.com)# bind http RS1 http
ServerIronADXB(config-vs-www.brocade.com)# bind http RS2 http
ServerIronADXB(config-vs-www.brocade.com)# exit
```

Syntax: [no] bind *<port> <real server name> <port>*

Enabling FWLB-to-SLB

To enable FWLB-to-SLB, enter the following command on the internal ServerIron ADX (ServerIron ADX B).

```
ServerIronADXB(config)# server fw-slb
```

Syntax: [no] server fw-slb

Configuration example for FWLB-to-SLB

The following sections show all the ServerIron commands you would enter on each ServerIron ADX to implement the FWLB-to-SLB configuration shown in .

Commands on ServerIron A (external)

The following commands change the ServerIron's host name to "ServerIronA", configure the ServerIron ADX's management IP address, and specify the default gateway.

```
ServerIronADX(config)# hostname ServerIronA
ServerIronADXA(config)# ip address 192.168.1.100 255.255.255.0
ServerIronADXA(config)# ip default-gateway 192.168.1.1
```

Enter the following commands to add two firewalls, FW1-IPin and FW2-IPin.

```
ServerIronADXA(config)# server fw-name FW1-IPin 192.168.1.30
ServerIronADXA(config-rs-FW1-IPin)# exit
ServerIronADXA(config)# server fw-name FW2-IPin 192.168.1.40
ServerIronADXA(config-rs-FW2-IPin)# exit
```

The following commands configure parameters for firewall group 2. The **fwall-info** commands configure the paths for the firewall traffic. Each path consists of a path ID, the ServerIron ADX port attached to the firewall, the IP address of the ServerIron ADX at the other end of the path, and the next-hop IP address (usually the firewall interface connected to this ServerIron ADX). Make sure you configure reciprocal paths on the other ServerIron ADX, as shown in the section containing the CLI commands for ServerIron ADX B.

NOTE
Path information is required even if the firewalls are synchronized.

The **fw-name** *<firewall-name>* command adds the firewalls to the firewall group.

```
ServerIronADXA(config)# server fw-group 2
ServerIronADXA(config-fw-2)# fw-name FW1-IPin
ServerIronADXA(config-fw-2)# fw-name FW2-IPin
ServerIronADXA(config-fw-2)# fwall-info 1 3 192.168.2.200 192.168.1.30
ServerIronADXA(config-fw-2)# fwall-info 2 5 192.168.2.200 192.168.1.40
ServerIronADXA(config-fw-2)# exit
```

The following commands add static MAC entries for the MAC addresses of the firewall interfaces connected to the ServerIron ADX. Notice that the QoS priority is configured as **priority 1** and the **router-type** parameter is specified. These parameters are required.

NOTE

To ensure proper operation, always configure the path IDs so that the IDs consistently range from lowest path ID to highest path ID for the firewalls. For example, in Figure 21 on page 137, the path IDs should range from lowest to highest beginning with the firewall interface at the upper left of the figure.

To ensure smooth operation, you might want to depict your firewalls in a vertical hierarchy as in Figure 21 on page 137, label the interfaces with their IP addresses, then configure the paths so that the path IDs to the interfaces range from lowest to highest path ID starting from the uppermost firewall interface.

```
ServerIronADXA(config)# static-mac-address abcd.4321.34e0 ethernet 3 priority 1
router-type
ServerIronADXA(config)# static-mac-address abcd.4321.34e1 ethernet 5 priority 1
router-type
ServerIronADXA(config)# write memory
```

Commands on ServerIron B (internal)

Enter the following commands to configure SLB. In an FWLB-to-SLB configuration, all SLB configuration takes place on the internal ServerIron ADX (ServerIron ADX B, the internal ServerIron ADX, in this example).

The following commands change the ServerIron ADX's host name to "ServerIron ADXB", configure the ServerIron ADX's management IP address, and specify the default gateway.

```
ServerIronADX(config)# hostname ServerIronADXB
ServerIronADXB(config)# ip address 192.168.2.200 255.255.255.0
ServerIronADXB(config)# ip default-gateway 192.168.2.1
```

The following commands configure the real servers. Notice that the servers are configured as local servers instead of remote servers. You can configure the real servers as local servers if Proxy ARP is enabled on the internal router.

```
ServerIronADXB(config)# server real-name RS1 192.168.2.50
ServerIronADXB(config-rs-RS1)# port http
ServerIronADXB(config-rs-RS1)# exit
ServerIronADXB(config)# server real-name RS2 192.168.2.60
ServerIronADXB(config-rs-RS2)# port http
ServerIronADXB(config-rs-RS2)# exit
```

The following commands configure the virtual server and bind it to the real servers with TCP port 80 (HTTP).

```
ServerIronADXB(config)# server virtual-name www.brocade.com
192.168.1.2ServerIronADX
ServerIronADXB(config-vs-www.brocade.com)# port http
```

```
ServerIronADXB(config)# server virtual www.brocade.com
ServerIronADXB(config-vs-www.brocade.com)# bind http RS1 http
ServerIronADXB(config-vs-www.brocade.com)# bind http RS2 http
```

Enter the following command to enable FWLB-to-SLB.

NOTE
This command applies only to the ServerIron ADX that contains the SLB configuration. Do not enter this command on the Internet ServerIron ADX (ServerIron ADXA).

```
ServerIronADXB(config)# server fw-slb
```

Enter the following commands to complete the FWLB configuration on this ServerIron ADX. Notice that the **fwall-info** commands configure paths that are reciprocal to the paths configured on ServerIron ADX A. Path 1 on each ServerIron ADX goes through one of the firewalls while path 2 goes through the other firewall.

```
ServerIronADXB(config)# server fw-name FW1-IPout 192.168.2.30
ServerIronADXB(config-rs-FW1-IPout)# exit
ServerIronADXB(config)# server fw-name FW2-IPout 192.168.2.40
ServerIronADXB(config-rs-FW2-IPout)# exit
ServerIronADXB(config)# server fw-group 2
ServerIronADXB(config-fw-2)# fw-name FW1-IPout
ServerIronADXB(config-fw-2)# fw-name FW2-IPout
ServerIronADXB(config-fw-2)# fwall-info 1 1 192.168.1.100 192.168.2.30
ServerIronADXB(config-fw-2)# fwall-info 2 2 192.168.1.100 192.168.2.40
ServerIronADXB(config-fw-2)# exit
ServerIronADXB(config)# static-mac-address abcd.4321.34e2 ethernet 1 priority 1
router-type
ServerIronADXB(config)# static-mac-address abcd.4321.34e3 ethernet 2 priority 1
router-type
ServerIronADXB(config)# write memory
```

Active-active FWLB – with external SLB (FWLB-to-SLB)

The software supports two types of FWLB with SLB configurations. Your choice of implementation depends on which pair of ServerIron ADXs you want to use for the SLB configuration. Use SLB-to-FWLB is you want to place the SLB configuration on the external ServerIron ADXs. Use FWLB-to-SLB if you want to place the SLB configuration on the internal ServerIron ADXs.

The software supports the following configurations:

- FWLB-to-SLB – The internal ServerIron ADX (the one on the server side or private side of the firewalls) contains all the SLB configuration information. In this configuration, the FWLB-to-SLB feature is enabled on the internal ServerIron ADX rather than the external ServerIron ADX. This configuration enables the internal ServerIron ADX to learn the firewall from which a client request is received and send the server reply back through the same firewall.

- SLB-to-FWLB – The external ServerIron ADX, on the client or external side of the firewalls, performs FWLB for traffic directed toward real servers connected to the ServerIron ADX on the private side of the firewalls. In this configuration, all the SLB configuration (virtual IP address, real server, and port bindings) resides on the external ServerIron ADX. The real servers are configured as remote servers. In addition, the SLB-to-FWLB feature is enabled on the external ServerIron ADX. The internal ServerIron is configured for FWLB but requires no additional configuration.

Figure 22 shows an example of an active-active FWLB configuration that also supports SLB. The pair of ServerIron ADXs on the non-secure (external) of the firewalls are connected to clients. The pair of ServerIron ADXs on the secure side of the firewalls are connected to application servers. Both pairs of ServerIron ADXs load balance the traffic to the firewalls and also perform SLB load balancing for application traffic.

Both ServerIron ADXs in each pair actively load balance traffic as well as provide redundancy.

You can configure the network in Figure 22 for FWLB-to-SLB or SLB-to-FWLB. The configuration commands after the figure show how to configure SLB-to-FWLB.

FIGURE 22   Active-active FWLB with SLB
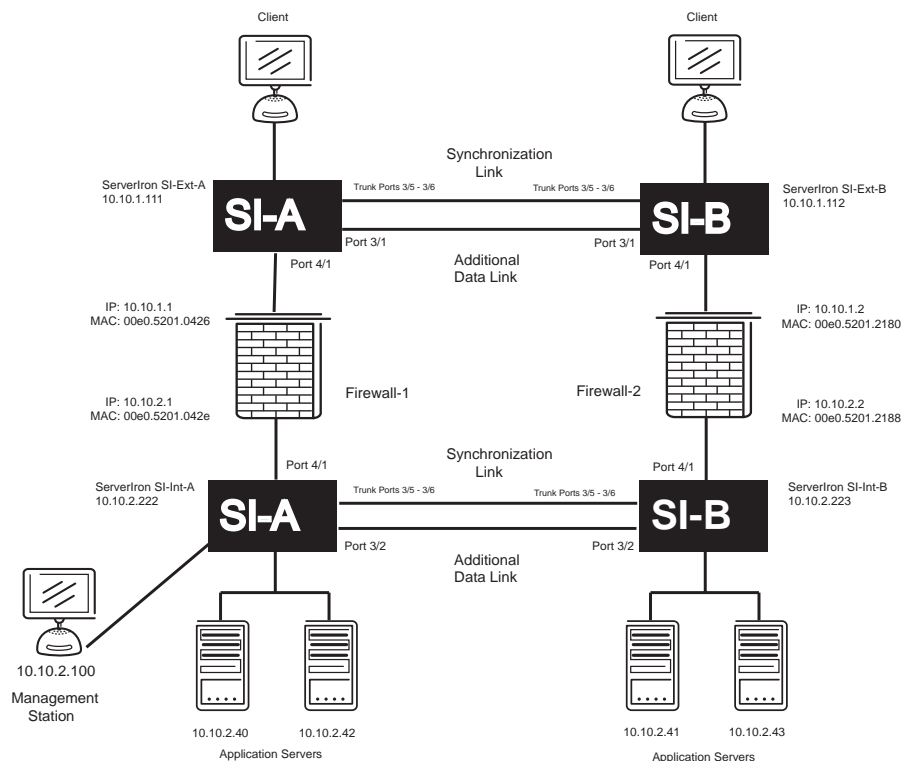
The CLI commands in this section show how to configure SLB-to-FWLB. In SLB-to-FWLB, the ServerIron ADX on the Internet side of the firewalls performs FWLB for traffic directed toward real servers connected to the ServerIron ADX on the private side of the firewalls. The real servers are configured as remote servers. In addition, the SLB-to-FWLB feature is enabled on the Internet ServerIron ADX. The internal ServerIron ADX is configured for FWLB but requires no additional configuration.

Commands on external ServerIron A (SI-Ext-A)

The following commands change the CLI to the global CONFIG level, then change the host name to "SI-Ext-A".

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-A
```

The following command enable the always-active feature and disables the Spanning Tree Protocol (STP) in VLAN 1, which contains the ports that will carry the FWLB traffic.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# always-active
SI-Ext-A(config-vlan-1)# no spanning-tree
```

The following commands configure a virtual routing interface on VLAN 1 (the default VLAN), then configure an IP address on the interface. The virtual routing interface is associated with all the ports in the VLAN.

```
SI-Ext-A(config-vlan-1)# router-interface ve 1
SI-Ext-A(config-vlan-1)# exit
SI-Ext-A(config)# interface ve 1
SI-Ext-A(config-ve-1)# ip address 10.10.1.111 255.255.255.0
SI-Ext-A(config-ve-1)# exit
```

The following command configures an IP default route. The next hop for this route is the ServerIron ADX's interface with firewall FW1.

```
SI-Ext-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
```

The following commands configure the dedicated synchronization link between the ServerIron ADX and its active-active partner. The **trunk** command configures the two ports of the link into a trunk group. The next two commands add the trunk group to a separate port-based VLAN, since the synchronization link must be in its own VLAN. The **server fw-port** command identifies the port number the link is on. If the link is a trunk group, you must specify the MAC address of the group's primary port.

```
SI-Ext-A(config)# trunk switch ethernet 3/5 to 3/6
SI-Ext-A(config)# trunk deploy
SI-Ext-A(config)# vlan 10
SI-Ext-A(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Ext-A(config-vlan-10)# exit
SI-Ext-A(config)# server fw-port 3/5
```

The following command configures the data link between this ServerIron ADX and its active-active partner. You must use the **server partner-ports** command to specify all the data links with the partner. However, do not use the command for the synchronization link.

```
SI-Ext-A(config)# server partner-ports ethernet 3/1
```

The following commands add the firewall definitions. In this example, port HTTP is specified for each firewall. Specifying the application ports on the firewalls is optional. The **port http no-health-check** command under each firewall disables the Layer 4 health check for the HTTP port. When you add an application port to a firewall definition, the ServerIron ADX automatically enables the Layer 4 health check for that port. You must disable the Layer 4 health check if the firewall is unable to act as a proxy for the application and respond to the health check. If the firewall does not respond to the health check, the ServerIron ADX assumes that the port is unavailable and stops sending traffic for the port to the firewall.

The ServerIron ADX will still use a Layer 3 health check (IP ping) to test connectivity to the firewall.

```
SI-Ext-A(config)# server fw-name fw1 10.10.1.1
SI-Ext-A(config-rs-fw1)# port http
SI-Ext-A(config-rs-fw1)# port http no-health-check
SI-Ext-A(config-rs-fw1)# exit
SI-Ext-A(config)# server fw-name fw2 10.10.1.2
SI-Ext-A(config-rs-fw2)# port http
SI-Ext-A(config-rs-fw2)# port http no-health-check
SI-Ext-A(config-rs-fw2)# exit
```

The following commands add the firewall definitions to the firewall port group (always group 2). The firewall group contains all the ports in VLAN 1 (the default VLAN).

```
SI-Ext-A(config)# server fw-group 2
SI-Ext-A(config-fw-2)# fw-name fw1
SI-Ext-A(config-fw-2)# fw-name fw2
```

The following command enables the active-active mode.

```
SI-Ext-A(config-fw-2)# sym-priority 1
```

NOTE
Do not use the same number on both ServerIrons. For example, enter **sym-priority 1** on one of the ServerIron ADXs and **sym-priority 255** on the other ServerIron.

The following commands add the paths through the firewalls to the other ServerIron ADX. Each path consists of a path number, a ServerIron ADX port number, the IP address at the other end of the path, and the next-hop IP address. In this example, the topology does not contain routers other than the ServerIron ADXs. If your topology does contain other routers, configure firewall paths for the routers too. For router paths, use the same IP address as the path destination and the next hop.

NOTE
The path IDs must be in contiguous, ascending numerical order, starting with 1. For example, path sequence 1, 2, 3, 4 is valid. Path sequence 4, 3, 2, 1 or 1, 3, 4, 5 is not valid.

```
SI-Ext-A(config-fw-2)# fwall-info 1 4/1 10.10.2.222 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 2 3/1 10.10.2.222 10.10.1.2
SI-Ext-A(config-fw-2)# fwall-info 3 4/1 10.10.2.223 10.10.1.1
SI-Ext-A(config-fw-2)# fwall-info 4 3/1 10.10.2.223 10.10.1.2
```

The following command sets the load balancing method to balance requests based on the firewall that has the least number of connections for the requested service. Since the firewall definitions above specify the HTTP service, the ServerIron ADX will load balance requests based on the firewall that has fewer HTTP session entries in the ServerIron ADX session table.

```
SI-Ext-A(config-fw-2)# fw-predictor per-service-least-conn
```

The following command is part of the always-active feature, which provides the additional data link between the this ServerIron ADX and its partner.

```
SI-Ext-A(config-fw-2)# l2-fwall
SI-Ext-A(config-fw-2)# exit
```

The following commands add static MAC entries for the firewall interfaces with the ServerIron ADX. The static MAC entries are required only if the configuration uses static routes and a single virtual routing interface, as in this example, and if the default gateway for the client or server is the firewall. If the configuration uses a dynamic routing protocol (for example, RIP or OSPF), the static entries are not required. Alternatively, the static entries are not required if you use the ServerIron itself as the default gateway for the client or the server. For example, the static entries are not required if you configure the client to use 10.10.1.111 as its default gateway.

```
SI-Ext-A(config)# vlan 1
SI-Ext-A(config-vlan-1)# static-mac-address 00e0.5201.0426 ethernet 4/1
priority 1 router-type
SI-Ext-A(config-vlan-1)# static-mac-address 00e0.5201.2180 ethernet 3/1
priority 1 router-type
SI-Ext-A(config-vlan-1)# exit
```

The following commands configure the SLB parameters, four real servers and one VIP. The servers are bound to the VIP by the HTTP port. Notice that the servers are configured as remote servers. If Proxy ARP is enabled on the internal ServerIron ADXs, you can define the real servers as local servers instead of remote servers. However, if Proxy ARP is not enabled on the internal ServerIron ADXs, the real servers must be remote servers.

```
SI-Ext-A(config)# server remote-name web1 10.10.2.40
SI-Ext-A(config-rs-web1)# port http
SI-Ext-A(config-rs-web1)# server remote-name web2 10.10.2.41
SI-Ext-A(config-rs-web2)# port http
SI-Ext-A(config-rs-web2)# server remote-name web3 10.10.2.42
SI-Ext-A(config-rs-web3)# port http
SI-Ext-A(config-rs-web3)# server remote-name web4 10.10.2.43
SI-Ext-A(config-rs-web4)# port http
SI-Ext-A(config-rs-web4)# server virtual webby 10.10.1.10
SI-Ext-A(config-vs-webby)# port http
SI-Ext-A(config-vs-webby)# bind http web4 http web3 http web2 http web1 http
```

Enter the following command to enable SLB-to-FWLB.

NOTE
This command applies only to the ServerIrons that contain the SLB configuration. Do not enter this command on the internal ServerIrons.

```
SI-Ext-A(config)# server slb-fw
SI-Ext-A(config)# write memory
```

Commands on external ServerIron B (SI-Ext-B)

Here are the commands for configuring SI-Ext-B in Figure 22 on page 146. The SLB configuration is identical to the one on SI-Ext-A.

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Ext-B
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# always-active
SI-Ext-B(config-vlan-1)# no spanning-tree
SI-Ext-B(config-vlan-1)# router-interface ve 1
SI-Ext-B(config-vlan-1)# exit
SI-Ext-B(config)# interface ve 1
SI-Ext-B(config-ve-1)# ip address 10.10.1.112 255.255.255.0
SI-Ext-B(config-ve-1)# exit
SI-Ext-B(config)# ip route 0.0.0.0 0.0.0.0 10.10.1.1
SI-Ext-B(config)# trunk switch ethernet 3/5 to 3/6
SI-Ext-B(config)# trunk deploy
SI-Ext-B(config)# vlan 10
SI-Ext-B(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Ext-B(config-vlan-10)# exit
SI-Ext-B(config)# server fw-port 3/5
SI-Ext-B(config)# server partner-ports ethernet 3/1
SI-Ext-B(config)# server fw-name fw1 10.10.1.1
SI-Ext-B(config-rs-fw1)# port http
SI-Ext-B(config-rs-fw1)# port http no-health-check
SI-Ext-B(config-rs-fw1)# exit
SI-Ext-B(config)# server fw-name fw2 10.10.1.2
SI-Ext-B(config-rs-fw2)# port http
SI-Ext-B(config-rs-fw2)# port http no-health-check
SI-Ext-B(config-rs-fw2)# exit
```

```
SI-Ext-B(config)# server fw-group 2
SI-Ext-B(config-fw-2)# fw-name fw1
SI-Ext-B(config-fw-2)# fw-name fw2
SI-Ext-B(config-fw-2)# sym-priority 255
SI-Ext-B(config-fw-2)# fwall-info 1 3/1 10.10.2.222 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 2 4/1 10.10.2.222 10.10.1.2
SI-Ext-B(config-fw-2)# fwall-info 3 3/1 10.10.2.223 10.10.1.1
SI-Ext-B(config-fw-2)# fwall-info 4 4/1 10.10.2.223 10.10.1.2
SI-Ext-B(config-fw-2)# fw-predictor per-service-least-conn
SI-Ext-B(config-fw-2)# l2-fwall
SI-Ext-B(config-fw-2)# exit
SI-Ext-B(config)# vlan 1
SI-Ext-B(config-vlan-1)# static-mac-address 00e0.5201.0426 ethernet 3/1
priority 1 router-type
SI-Ext-B(config-vlan-1)# static-mac-address 00e0.5201.2180 ethernet 4/1
priority 1 router-type
SI-Ext-B(config-vlan-1)# exit
SI-Ext-B(config)# server remote-name web1 10.10.2.40
SI-Ext-B(config-rs-web1)# port http
SI-Ext-B(config-rs-web1)# server remote-name web2 10.10.2.41
SI-Ext-B(config-rs-web2)# port http
SI-Ext-B(config-rs-web2)# server remote-name web3 10.10.2.42
SI-Ext-B(config-rs-web3)# port http
SI-Ext-B(config-rs-web3)# server remote-name web4 10.10.2.43
SI-Ext-B(config-rs-web4)# port http
SI-Ext-B(config-rs-web4)# server virtual webby 10.10.1.10
SI-Ext-B(config-vs-webby)# port http
SI-Ext-B(config-vs-webby)# bind http web4 http web3 http web2 http web1 http
SI-Ext-B(config)# server slb-fw
SI-Ext-B(config)# write memory
```

Commands on internal ServerIron A (SI-Int-A)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-A
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# always-active
SI-Int-A(config-vlan-1)# no spanning-tree
SI-Int-A(config-vlan-1)# router-interface ve 1
SI-Int-A(config-vlan-1)# exit
SI-Int-A(config)# interface ve 1
SI-Int-A(config-ve-1)# ip address 10.10.2.222 255.255.255.0
SI-Int-A(config-ve-1)# exit
SI-Int-A(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.1
SI-Int-A(config)# trunk switch ethernet 3/5 to 3/6
SI-Int-A(config)# trunk deploy
SI-Int-A(config)# vlan 10
SI-Int-A(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Int-A(config-vlan-10)# exit
SI-Int-A(config)# server fw-port 3/5
SI-Int-A(config)# server partner-ports ethernet 3/2
SI-Int-A(config)# server fw-name fw1 10.10.2.1
SI-Int-A(config-rs-fw1)# port http
SI-Int-A(config-rs-fw1)# port http no-health-check
SI-Int-A(config-rs-fw1)# exit
SI-Int-A(config)# server fw-name fw2 10.10.2.2
SI-Int-A(config-rs-fw2)# port http
SI-Int-A(config-rs-fw2)# port http no-health-check
```

```
SI-Int-A(config-rs-fw2)# exit
SI-Int-A(config)# server fw-group 2
SI-Int-A(config-fw-2)# fw-name fw1
SI-Int-A(config-fw-2)# fw-name fw2
SI-Int-A(config-fw-2)# sym-priority 1
SI-Int-A(config-fw-2)# fwall-info 1 4/1 10.10.1.111 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 2 3/2 10.10.1.111 10.10.2.2
SI-Int-A(config-fw-2)# fwall-info 3 4/1 10.10.1.112 10.10.2.1
SI-Int-A(config-fw-2)# fwall-info 4 3/2 10.10.1.112 10.10.2.2
SI-Int-A(config-fw-2)# fw-predictor per-service-least-conn
SI-Int-A(config-fw-2)# l2-fwall
SI-Int-A(config-fw-2)# exit
SI-Int-A(config)# vlan 1
SI-Int-A(config-vlan-1)# static-mac-address 00e0.5201.042e ethernet 4/1
priority 1 router-type
SI-Int-A(config-vlan-1)# static-mac-address 00e0.5201.2188 ethernet 3/2
priority 1 router-type
SI-Int-A(config-vlan-1)# exit
SI-Int-A(config)# write memory
```

Commands on internal ServerIron B (SI-Int-B)

```
ServerIronADX> enable
ServerIronADX# configure terminal
ServerIronADX(config)# hostname SI-Int-B
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# always-active
SI-Int-B(config-vlan-1)# no spanning-tree
SI-Int-B(config-vlan-1)# router-interface ve 1
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# interface ve 1
SI-Int-B(config-ve-1)# ip address 10.10.2.223 255.255.255.0
SI-Int-B(config-ve-1)# exit
SI-Int-B(config)# ip route 0.0.0.0 0.0.0.0 10.10.2.2
SI-Int-B(config)# trunk switch ethernet 3/5 to 3/6
SI-Int-B(config)# trunk deploy
SI-Int-B(config)# vlan 10
SI-Int-B(config-vlan-10)# untagged ethernet 3/5 to 3/6
SI-Int-B(config-vlan-10)# exit
SI-Int-B(config)# server fw-port 3/5
SI-Int-B(config)# server partner-ports ethernet 3/2
SI-Int-B(config)# server fw-name fw1 10.10.2.1
SI-Int-B(config-rs-fw1)# port http
SI-Int-B(config-rs-fw1)# port http no-health-check
SI-Int-B(config-rs-fw1)# exit
SI-Int-B(config)# server fw-name fw2 10.10.2.2
SI-Int-B(config-rs-fw2)# port http
SI-Int-B(config-rs-fw2)# port http no-health-check
SI-Int-B(config-rs-fw2)# exit
SI-Int-B(config)# server fw-group 2
SI-Int-B(config-fw-2)# fw-name fw1
SI-Int-B(config-fw-2)# fw-name fw2
SI-Int-B(config-fw-2)# sym-priority 255
SI-Int-B(config-fw-2)# fwall-info 1 3/2 10.10.1.111 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 2 4/1 10.10.1.111 10.10.2.2
SI-Int-B(config-fw-2)# fwall-info 3 3/2 10.10.1.112 10.10.2.1
SI-Int-B(config-fw-2)# fwall-info 4 4/1 10.10.1.112 10.10.2.2
SI-Int-B(config-fw-2)# fw-predictor per-service-least-conn
SI-Int-B(config-fw-2)# l2-fwall
```

```
SI-Int-B(config-fw-2)# exit
SI-Int-B(config)# vlan 1
SI-Int-B(config-vlan-1)# static-mac-address 00e0.5201.042e ethernet 3/2
priority 1 router-type
SI-Int-B(config-vlan-1)# static-mac-address 00e0.5201.2188 ethernet 4/1
priority 1 router-type
SI-Int-B(config-vlan-1)# exit
SI-Int-B(config)# write memory
```

Supporting dual homed servers in FWLB design

In Figure 23, the internal server is dual homed and uses active-standby NICs. VRRP Extended (VRRP-E) is configured on both Internal ServerIron ADX A and Internal ServerIron ADX B. Internal ServerIron A is the VRRP-E master, while internal ServerIron B is the VRRP-E backup. (Refer to the "Configuring VRRP and VRRP-E" chapter of the *ServerIron ADX Switch and Router Guide* for information on VRRP-E.)

The server NIC that connects to the VRRP-E master ServerIron ADX is active and the one that connects to the VRRP-E backup ServerIron ADX is standby.

FIGURE 23   Example of server with two NICs
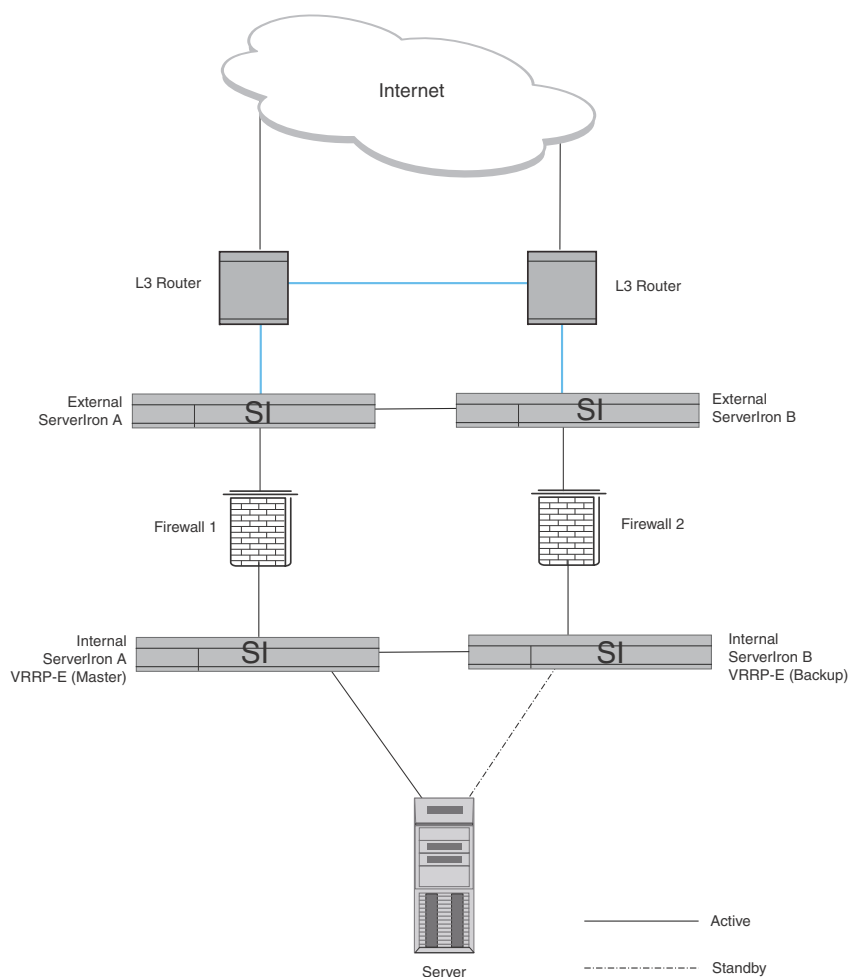
Consider a failure situation where the link between Firewall-1 and External ServerIron ADX-A has failed. All four ServerIron ADXs will detect this firewall path failure. Also, assume that the active NIC on the internal server has failed and the standby NIC has taken over. The VRRP-E ownership on the internal ServerIron ADXs however will not change as this VRRP-E instance is not tracking server side interfaces.

The ingress traffic which arrives in External ServerIron A will be forwarded to the internal server through External ServerIron ADX B, Firewall-2 and Internal ServerIron ADX B. The response traffic will first arrive at the Internal ServerIron ADX B through the "currently active" standby NIC. Since this traffic would be destined to the VRRP-E address, the internal ServerIron ADX B forwards it to Internal ServerIron A over the firewall partner port. Upon receiving this traffic over the partner port, the Internal ServerIron ADX A forwards it at Layer 3 to Firewall-1 which then drops the traffic as it won't have an exit path.

Enabling the **server fw-force-route** command helps address this situation. Enable this command on both Internal ServerIron units in order to prevent traffic failure.

```
Internal ServerIronADXA(config)#server fw-force-route
Internal ServerIronADXB(config)#server fw-force-route
```

Syntax: [no] server fw-force-route

Viewing FWLB Configuration Details and Statistics

In this chapter

FWLB configuration overview

You can view the following FWLB configuration details and statistics:

- Firewall group information – Displays the firewall configuration, the status of each firewall, and traffic statistics for traffic between each firewall and the ServerIron ADX.

- Firewall path information – Shows the synchronization paths configured for the firewall.

- Hashing information – Shows the firewall selected by the hashing algorithm for a given pair of source and destination addresses.

Displaying firewall group information

To display configuration information, state information, and traffic statistics for the firewall group, use the following CLI method.

To access FWLB configuration details and statistics, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show fw-group
```

This command shows the following information. To explain the output, this example is divided into sections. The output is not divided in this way on the screen of your management terminal.

The first line indicates the firewall group and the number of firewalls in the group. This firewall group is group number 2 (IPv4) and contains two firewalls. The second line shows the source and destination values for the hash mask.

```
Firewall-group 2 has 2 members Admin-status = Enabled
Hash_info: Dest_mask = 255.255.255.255 Src_mask = 255.255.255.255
```

The following lines list the firewalls configured in the firewall group, show the administrative state, and have distribution values for each firewall:

- The administrative state is shown in the Admin-st column and depends on the results of the Layer 3 health check (ping) the ServerIron performs when you add the path information for the firewall. The administrative state can be one of the following:
  - **0** – Disabled
  - **1** – Enabled
  - **2** – Failed
  - **3** – Testing
  - **4** – Suspect
  - **6** – Active

NOTE
Status 5 (Graceful Shutdown) does not apply to firewalls.

- The Hash-distribution field shows how many hash values are assigned to the server. This information is relevant only when no path information is configured for the firewall group. If the group is using paths, the hash-distribution value is always 0.

```
Firewall Server Name             Admin-st   Hash-distribution
fw1                                 1                   0
fw2                                 6                   0
```

The following lines show traffic statistics for each firewall. The Name field lists the name of the firewall and the IP field shows the IP address of the firewall. The "Host" indicates the ServerIron ADX. The "Firewall" indicates the firewall. The Groups field shows the firewall group number.

The statistics are for traffic between the ServerIron ADX and the firewall. The CurConn and TotConn columns show the total number of connections between the ServerIron ADX and the firewall. A connection represents both send and receive traffic. (Thus, each connection shown here is equivalent to two sessions.) The Packets and Octets fields show the total number of packets and octets exchanged by the ServerIron ADX and the firewall.

```
Traffic From<->to Firewall Servers
===================================

Name: fw1              IP: 10.10.0.1        State: 1   Groups =   2

                                      Host->Firewall        Firewall->Host
            State CurConn TotConn    Packets     Octets    Packets     Octets
Default     active    0       0         0          0          0          0
Total                 0       0         0          0          0          0

Name: fw2              IP: 10.10.0.2        State: 6   Groups =   2

                                      Host->Firewall        Firewall->Host
            State CurConn TotConn    Packets     Octets    Packets     Octets
Default     active    0       0         0          0          0          0
Total                 0       0         0          0          0          0
```

The following example shows firewall group 4 (IPv6) and contains two firewalls.

```
Firewall-group 4 has 2 members Admin-status = Enabled Active = 0

Hash_info: Dest_mask = ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Src_mask = ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Firewall Server Name   Admin-status   Hash-distribution
v6fw1                  6              0        0
v6fw2                  6              0        0


Traffic From<->to Firewall Servers
Name: v6fw1            IP6: 33::3                          State: 6 Groups = 4
                                      Host->Firewall   Firewall->Host
           State    CurCon  TotCon  Packets  Octets  Packets  Octets
Default    active   1       1       25       1947    0        0
In-default active   0       4       0        0       0        0
Total               1       5       25       1947    0        0


Name: v6fw2            IP6: 33::4                          State: 6 Groups = 4
                                      Host->Firewall   Firewall->Host
           State    CurCon  TotCon  Packets  Octets  Packets  Octets
Default    active   0       0       106      7969    719      67119
In-default active   0       6       0        0       9007     757666
Total               0       6       106      7969    9726     824785
```

TCP/UDP port statistics

If you associated TCP/UDP application ports with specific firewalls (part of a stateful FWLB configuration), rows of statistics for the application ports also are listed. The following example shows statistics for two ServerIron ADXs in a basic stateful FWLB configuration. In this example, HTTP traffic and Telnet traffic are explicitly associated with fw1 and fw2.

```
ServerIronADXA(config)# show fw-group
Firewall-group 2 has 2 members Admin-status = Enabled Active = 0
Hash_info: Dest_mask = 255.255.255.255 Src_mask = 255.255.255.255

Firewall Server Name              Admin-status Hash-distribution
fw1-IPin                          6            0
fw2-IPin                          6            0

Traffic From<->to Firewall Servers

Name: fw1-IPin          IP: 209.157.22.3      State: 6    Groups =    2

                                  Host->Fw-Server      Fw-Server->Host
          State   CurConn TotConn Packets    Octets    Packets    Octets
http      active  8       37445   264015     18232357  326241     339770826
In-http   active  0       0       0          0         0          0
telnet    active  0       0       0          0         0          0
In-telnet active  0       0       0          0         0          0
Fw-Server active  0       0       0          0         21         2384
Total             8       37445   264015     18232357  326262     339773210

Name: fw2-IPin        IP: 209.157.22.4      State: 6    Groups =    2

                                  Host->Fw-Server      Fw-Server->Host
          State   CurConn TotConn Packets    Octets    Packets    Octets
http      active  8       30655   216957     14977685  110028     114839282
In-http   active  0       0       0          0         0          0
telnet    active  0       0       0          0         0          0
In-telnet active  0       0       0          0         0          0
Fw-Server active  0       0       0          0         25         2912
Total             8       30655   216957     14977685  110053     114842194
```

The "**http**" and "**telnet**" rows show statistics for traffic initiated by clients or servers. The "**In-http**" and "**In-telnet**" rows show statistics for replies. In the example shown above, the statistics indicate requests from clients outside the firewalls sent to servers on the private side of the firewalls.

In general, a ServerIron ADX will show statistics for only one direction:

- If the ServerIron ADX is on the external (Internet) side of the firewalls, the ServerIron will show statistics in the "http" row, "telnet" row, and so on. For example, statistics for TCP SYN packets from clients are listed in the "http" row.

- If the ServerIron ADX is on the internal (private network) side of the firewalls, the ServerIron ADX will show statistics in the "In-http" row, "In-telnet" row, and so on. For example, server replies to TCP SYN packets from clients are listed in the "In-http" row.

The previous example is for the external ServerIron ADX (ServerIron A). The following example shows statistics for the internal ServerIron ADX (ServerIron ADX B).

```
ServerIronADXB(config)# show fw-group
Firewall-group 2 has 2 members Admin-status = Enabled Active = 0
Hash_info: Dest_mask = 255.255.255.255 Src_mask = 255.255.255.255

Firewall Server Name              Admin-status Hash-distribution
fw1-IPout                         6            0
fw2-IPout                         6            0

Traffic From<->to Firewall Servers
Name: fw1-IPout        IP: 209.157.23.1     State: 6    Groups =   2
                                   Host->Fw-Server      Fw-Server->Host
           State   CurConn TotConn Packets   Octets      Packets   Octets
http       active  0       0       0         0           0         0
In-http    active  3       11118   71054     74037240    78564     5422929
Fw-Server  active  0       0       0         0           0         0
Total              3       11118   71054     74037240    78564     5422929

Name: fw2-IPout        IP: 209.157.23.2     State: 6    Groups =   2
                                   Host->Fw-Server      Fw-Server->Host
           State   CurConn TotConn Packets   Octets      Packets   Octets
http       active  0       0       0         0           0         0
In-http    active  4       9182    59169     61874490    65057     4490977
Fw-Server  active  0       0       0         0           0         0
Total              4       9182    59169     61874490    65057     4490977
```

In this example, the ServerIron ADX shows statistics for server replies to client requests. The **show fw-group** command on the external ServerIron ADX (ServerIron A) shows the requests, while the **show fw-group** command on the internal ServerIron ADX (ServerIron ADX B), shows the server replies to those requests.

Displaying firewall path information

The ServerIron ADX uses paths that you configure to provide synchronization for the traffic that passes through the ServerIron ADXs and the Layer 3 firewalls between them. You can display configuration information, state information, and statistics for the paths using the following CLI command.

NOTE
The information is shown from this ServerIron ADX's perspective. To view the other side of the path configuration, display the firewall path information on the ServerIron ADX at the other end of the path.

To display path information for FWLB, enter the following command at any level of the CLI.

```
ServerIron_ADX(config)#show server fw-path

IPv4 Firewall Server Path Info

==============================

Number of Paths Configured      = 4

Number of Fwall Paths preferred       = 2

Number of Router Paths preferred      = 1

Target-ip      Next-hop-ip     Port          Path    Status Tx  Rx   State Zone
```

```
33.1.1.1      23.1.1.3        15              1       1       1   1   5       1
33.1.1.1      23.1.1.4        11              2       1       1   1   5       1
33.1.1.2      23.1.1.3        15              3       1       1   1   5       1
33.1.1.2      23.1.1.4        11              4       1       1   1   5       1
State = 5, Partner known = Yes, port = 14, sync-state = 0
FW Partner MAC        = 001b.ed05.ee20
              Current         Local           Partner
State         5               5               5
Priority      40              40              40
Path-cnt      4               4               4
Router-cnt    0               0               0
Active path cnt = 4, list =   1    2    3    4


IPv6 Firewall Server Path Info
==============================
Number of Paths Configured      = 5
Number of Fwall Paths preferred     = 2
Number of Router Paths preferred     = 1
Target-ipv6    Next-hop-ipv6    Port           Path    Status Tx  Rx  State Zone
33::1          23::3            15             1       1       1   1   5       1
33::1          23::4            11             2       1       1   1   5       1
33::2          23::3            15             3       1       1   1   5       1
33::2          23::4            11             4       1       1   1   5       1
15::2          15::2            9              5       1       1   1   5       1
State = 5, Partner known = Yes, port = 14, sync-state = 0
FW Partner MAC        = 001b.ed05.ee20
              Current         Local           Partner
State         5               5               5
Priority      40              40              40
Path-cnt      4               4               4
Active path cnt = 5, list =   1    2    3    4    5
```

Table 8 describes the information displayed by the **show server fw-path** command.

TABLE 8 FWLB path information

Field	Description
General Information	
Number of Paths Configured	The number of firewall and router paths configured in the group.
Number of Fwall Paths preferred	
Number of Router Paths preferred	
Target-ip (IPv4) Target-ipv6	The IP address of the device at the other end of the path. Generally, this other device is another ServerIron.
Next-hop-ip (IPv4) Next-hop-ipv6	The IP address of the device at the next hop to the target IP. Usually, this is the IP interface on the firewall that is connected to this ServerIron.
Port	The ServerIron port for this path. This is the port connected to the firewall.
Path	The path ID.
Status	The status of the path, which can be one of the following: • 0 – The path is down. • 1 – The path is up.
Tx	Indicates the state of the transmit side of the path. The state can be one of the following: • 0 – The transmit side is down. • 1 – The transmit side is up.
Rx	Indicates the state of the receive side of the path. The state can be one of the following: • 0 – The receive side is down. • 1 – The receive side is up.
State	The state of the other end of the path. 5 – The ServerIron ADX at the other end of the path is in active mode for the firewall group. **NOTE:** This field applies only to IronClad FWLB. If the ServerIron ADX is not configured with another ServerIron ADX as the active or backup ServerIron ADX for IronClad FWLB, the state is always 0.
Zone	
Partner known	Indicates whether this ServerIron ADX can see (has Layer 2 connectivity with) the other ServerIron ADX in the pair. This field can have one of the following values: • No – This ServerIron ADX does not have Layer 2 connectivity with its partner. Generally, this indicates that the link is down. • Yes – This ServerIron ADX has Layer 2 connectivity with its partner. **NOTE:** This field applies only to the other ServerIron ADX in an active-standby configuration for IronClad FWLB.
port	
sync-state	
FW Partner MAC valid	
FW Partner MAC	

TABLE 8 FWLB path information (Continued)

Field	Description
State (Current, Local, and Partner)	Current, local, and active state information for the path: • The current state indicates the immediate state information. This is the most current information. • The local state indicates the cumulative current states over a three-second interval. If the current states have been the same for the previous three seconds, the state is shown in the Local column. • The partner state. In each column, the state can be one of the following: • 0 – Unknown. Generally, this indicates that the link is down. • 5 – The ServerIron is in active mode for the firewall group.
Priority	The IronClad FWLB priority for the firewalls in the firewall group. The ServerIron ADX with the higher priority for the group ID the default active ServerIron ADX for the group.
Path-cnt	The number of firewall paths.
Router-cnt	
Active path cnt	The number of paths from this ServerIron ADX that go to active ServerIron ADXs. A path that goes to a ServerIron ADX that is in standby mode is not counted in this statistic.
list	A list of the configured paths.

Displaying the firewall selected by the hashing process for load balancing

By default, FWLB uses a hashing algorithm to select a firewall for a packet based on the packet's source and destination IP address. Optionally, you can configure the ServerIron ADX to also hash based on source and destination TCP or UDP application ports. Once the ServerIron ADX selects a firewall for a given pair of source and destination IP addresses (and, if specified, source and destination TCP or UDP application ports), the ServerIron always selects the same firewall for packets with the same address pairs.

To display the firewall that the hashing algorithm selected for a given pair of source and destination addresses, enter the following command.

```
ServerIronADX# show fw-hash 1.1.1.1 2.2.2.2 2
fw3
```

In this example, the command output indicates that the FWLB hashing algorithm selected firewall "fw3" for traffic to IP address 1.1.1.1 from IP address 2.2.2.2.

Syntax: **(IPv4) show fw-hash** *<dst-ip-addr> <src-ip-addr> <fwall-group-id>* [*<protocol> <dst-tcp/udp-port> <src-tcp/udp-port>*]

Syntax: **(IPv6) show fw-hash** *<dst-ipv6-addr> <src-ipv6-addr> <fwall-group-id>* [*<protocol> <dst-tcp/udp-port> <src-tcp/udp-port>*]

The *<dst-ip-addr>* parameter specifies the destination IPv4 address.

The *<src-ip-addr>* parameter specifies the source IPv4 address.

The *<dst-ipv6-addr>* parameter specifies the destination IPv6 address.

The *<src-ipv6-addr>* parameter specifies the source IPv6 address.

The *<fwall-group-id>* parameter specifies the FWLB group ID. For IPv4, the FWLB group ID is 2. For IPv6, the FWLB group ID is 4.

The *<protocol>* parameter specifies the protocol number for TCP or UDP. You can specify one of the following:

- 6 – TCP
- 17 – UDP

The *<dst-tcp/udp-port>* specifies the destination TCP or UDP application port number.

The *<src-tcp/udp-port>* specifies the source TCP or UDP application port number.

If you configured the ServerIron ADX to hash based on source and destination TCP or UDP application ports as well as IP addresses, the ServerIron ADX might select more than one firewall for the same pair of source and destination IP addresses, when the traffic uses different pairs of source and destination application ports. Use the optional parameters to ensure that the command's output distinguishes among the selected firewalls based on the application ports.

Here is an IPv4 example:

```
ServerIronADX# show fw-hash 1.1.1.1 2.2.2.2 2 6 80 8080
ServerIronADX# show fw-hash 1.1.1.1 2.2.2.2 2 6 80 9000
```

Here is an IPv6 example:

```
ServerIronADX# show fw-hash 33::1 33::2 4 6 80 8080
```

Additional Firewall Configurations

In this appendix

Configuring FWLB for firewalls with active-standby NICs

Some firewalls provide reliability through link redundancy. For example, some firewalls can have two NICs on each sub-net. One of the NICs is active. The other NIC is a standby interface and is used only if the active NIC becomes unavailable. Both NICs have the same IP address. You can use this type of firewall in IronClad configurations that use the always-active feature.

NOTE
The always-active feature enables you to simplify FWLB configuration by eliminating extra layers of Layer 2 switches. Refer to "Configuring the additional data link (the always-active link)" on page 43.

To configure a ServerIron ADX to load balance traffic for firewalls that use dual NICs for link redundancy, specify a wildcard value (65535) instead of a specific ServerIron ADX port number when you configure the paths to the firewall. When you add a firewall path, the ServerIron ADX sends an ARP request to obtain the MAC address of the next-hop IP address for the path, which in most configurations is the firewall NIC. If the ServerIron ADX port number for the path is a wildcard (65535), the ServerIron ADX also learns the port for the path, which is the port on which the ServerIron ADX receives the ARP reply from the NIC.

Figure 24 shows an example of an always-active configuration.

This configuration and the commands for implementing it are almost the same as for the configuration in "IronClad FWLB configuration with multi-homed firewalls" The only differences are as follows:

- Each firewall is connected to both ServerIron ADXs on each side of the network. For example, firewall FW1 is connected to both ServerIron SI-Ext-A and ServerIron SI-Ext-B. Each link has a unique MAC address but they use the same IP address. Only one of the links is active at a time. The other link is a standby.

- The firewall paths on each ServerIron use a wildcard value (65535) instead of a specific ServerIron port number.

FIGURE 24   FWLB configuration using always-active with active-standby firewall interfaces
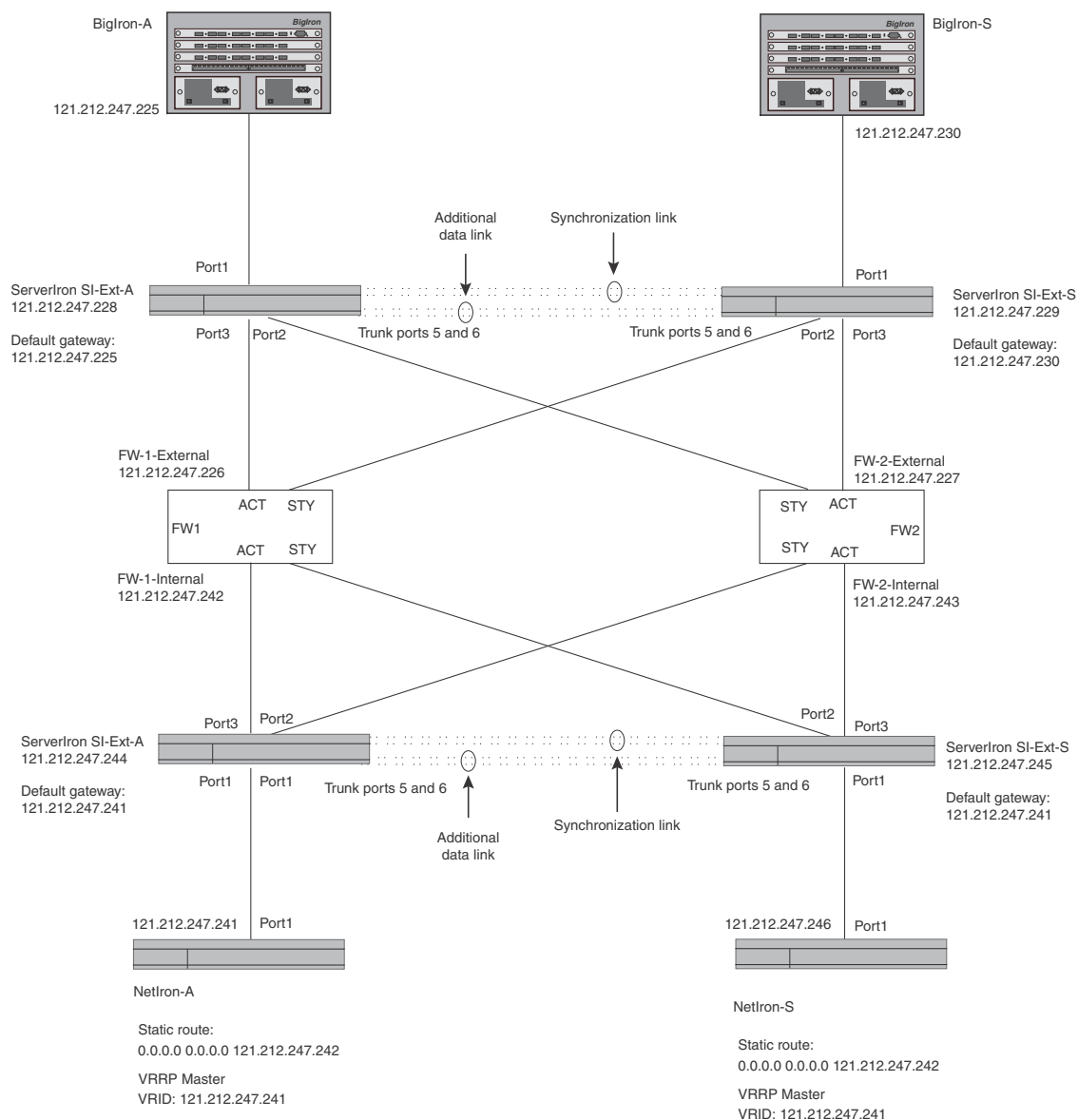
In this example, the links on each firewall are marked to indicate whether they are in the active (ACT) or standby (STY) state. The ServerIron ADX sends traffic to the active firewall interface but not to the standby interface. For example, ServerIron ADX SI-Ext-A sends traffic to firewall FW1 through port 3 because the firewall's link with the ServerIron ADX is on port 3. However, if the link becomes unavailable and the firewall fails over to the other link, ServerIron ADX SI-Ext-A can no longer reach the firewall through port 3. ServerIron ADX SI-Ext-A must use the additional data link configured on ports 5 and 6 (a trunk group in this configuration) to reach the firewall, by sending the traffic through ServerIron ADX SI-Ext-B. (The always-active feature enables the ServerIron ADXs in the active-standby pair to use each other as data paths in instances such as this.)

The ServerIron ADX has only one path to each firewall, but the path uses a wildcard for the ServerIron ADX port number. The ServerIron ADX determines the port to use for reaching the firewall by sending an ARP request for the firewall interface. When the active link on the firewall responds with its MAC address, the ServerIron ADX learns the port on which the response is received and uses that port to reach the firewall.

If the firewall link goes down and the NIC fails over to the other connection, the ServerIron ADX learns the new port for the MAC address. Generally, this occurs when the NIC sends a gratuitous ARP to advertise the new MAC address. The ServerIron ADX learns that the link has failed when the firewall path health check fails. The path health check consists of an IP ping to the next-hop IP address of the path.

Configuring for active-standby firewall links

To configure firewall paths for firewalls with active-standby NICs, enter commands such as the following. Notice that the first four paths configured for each ServerIron ADX specify 65535 as the ServerIron ADX port number (the second parameter in the command). The last path is the path to the router and does use a specific ServerIron ADX port instead of the wildcard (65535).

Commands for active external ServerIron ADX (SI-Ext-A)

```
SI-Ext-A(config)# server fw-group 2
SI-Ext-A(config-fw-2)# fwall-info 1 65535 121.212.247.244 121.212.247.226
SI-Ext-A(config-fw-2)# fwall-info 2 65535 121.212.247.245 121.212.247.226
SI-Ext-A(config-fw-2)# fwall-info 3 65535 121.212.247.244 121.212.247.227
SI-Ext-A(config-fw-2)# fwall-info 4 65535 121.212.247.245 121.212.247.227
SI-Ext-A(config-fw-2)# fwall-info 5 1 121.212.247.225 121.212.247.225
```

Commands for standby external ServerIron ADX (SI-Ext-S)

```
SI-Ext-S(config)# server fw-group 2
SI-Ext-S(config-fw-2)# fwall-info 1 65535 121.212.247.244 121.212.247.226
SI-Ext-S(config-fw-2)# fwall-info 2 65535 121.212.247.245 121.212.247.226
SI-Ext-S(config-fw-2)# fwall-info 3 65535 121.212.247.244 121.212.247.227
SI-Ext-S(config-fw-2)# fwall-info 4 65535 121.212.247.245 121.212.247.227
SI-Ext-S(config-fw-2)# fwall-info 5 1 121.212.247.230 121.212.247.230
```

Commands for active internal ServerIron ADX (SI-Int-A)

```
SI-Int-A(config)# server fw-group 2
SI-Int-A(config-fw-2)# fwall-info 1 65535 121.212.247.228 121.212.247.242
SI-Int-A(config-fw-2)# fwall-info 2 65535 121.212.247.229 121.212.247.242
SI-Int-A(config-fw-2)# fwall-info 3 65535 121.212.247.228 121.212.247.243
SI-Int-A(config-fw-2)# fwall-info 4 65535 121.212.247.229 121.212.247.243
SI-Int-A(config-fw-2)# fwall-info 5 1 121.212.247.241 121.212.247.241
```

Commands for standby internal ServerIron ADX (SI-Int-S)

```
SI-Int-S(config)# server fw-group 2
SI-Int-S(config-fw-2)# fwall-info 1 65535 121.212.247.228 121.212.247.242
SI-Int-S(config-fw-2)# fwall-info 2 65535 121.212.247.229 121.212.247.242
SI-Int-S(config-fw-2)# fwall-info 3 65535 121.212.247.228 121.212.247.243
SI-Int-S(config-fw-2)# fwall-info 4 65535 121.212.247.229 121.212.247.243
SI-Int-S(config-fw-2)# fwall-info 5 1 121.212.247.246 121.212.247.246
```

Syntax: (IPv4) [no] **fwall-info** *<path-num> <portnum> <other-ip> <next-hop-ip>*

Syntax: (IPv6) [no] **fwall-info** *<path-num> <portnum> <other-ipv6> <next-hop-ipv6>*

NOTE
The other IP address and next-hop IP address parameters must be both IPv4 addresses or both IPv6 addresses. IPv4 and IPv6 addresses cannot be mixed.

NOTE
You must use IPv4 addresses for IPv4 firewalls and IPv6 addresses for IPv6 firewalls. If the same firewall supports both IPv4 and IPv6, you must configure them separately under group 2 (IPv4) and group 4 (IPv6).

The *<path-num>* parameter specifies the path. The sequence of path IDs must be contiguous from start to finish.

The *<portnum>* parameter specifies the port that connects the ServerIron to the firewall. If the port number is dynamic, use port number 65535.

The *<other-ip>* parameter specifies the IPv4 address of the ServerIron on the other side of the firewall.

The *<next-hop-ip>* parameter specifies the IPv4 address of the firewall connected to this ServerIron.

The *<other-ipv6>* parameter specifies the IPv6 address of the ServerIron on the other side of the firewall.

The *<next-hop-ipv6>* parameter specifies the IPv6 address of the firewall connected to this ServerIron.

Specify 65535 as the port number for the paths to dual NIC (active-standby) firewall interfaces. Specify the ServerIron ADX port number for paths to routers.

When the firewalls have active-standby NICs, and dynamic ports are configured on the firewall paths, by default the ServerIron always uses the same interface to reach a firewall, where firewall's ARP entry was initially learnt. It does not update the firewall path to an alternate interface unless the interface physically goes down.

This behavior will cause issues in setups running firewalls with active-standby NIC's, when the NICs fail over without having the interface go down physically. For example, when a failover of the Firewall NIC occurs, the ARP entry for the firewall's IP is learnt on a new port but the firewall path still shows the old interface causing issues with FWLB.

Configure the following command, to prevent this condition:

```
ServerIronADX(config)# server fw-allow-dynamic-port-change
```

Syntax: **server fw-allow-dynamic-port-change**

This command allows the firewall path health checks to be sent to the correct port where the firewall ARP is learnt and update the firewall path accordingly to reflect the new interface where the firewall can now be reached.

Customizing path health checks

This appendix describes the health checks for firewall and router paths and how to change their configuration.

By default, the ServerIron ADX checks the health of each firewall and router path by sending an ICMP ping on the path every 400 milliseconds. Consider the following to determine the router path:

- If the ServerIron ADX receives one or more responses within 1.2 seconds, the ServerIron ADX concludes that the path is healthy.

- Otherwise, the ServerIron ADX reattempts the health check by sending another ping. By default, the ServerIron ADX reattempts an unanswered path health check up to three times before concluding that the path is unhealthy.

You can change the maximum number of retries for the Layer 3 health checks of firewall and router paths. You also can enable Layer 4 path health checks for the firewall paths.

NOTE
This chapter describes how to configure path health checks but not application health checks. To configure a Layer 4 or Layer 7 application health check, use the procedures in the "Health Checks" chapter in the *ServerIron Server Load Balancing Guide*. The command syntax and behavior of Layer 4 and Layer 7 health checks is the same regardless of whether you are configuring them for SLB, TCS, or FWLB.

Changing the maximum number of Layer 3 path health-check retries

By default, the ServerIron ADX checks the health of each firewall and router path by sending an ICMP ping on the path every 400 milliseconds:

- If the ServerIron ADX receives one or more responses within 1.2 seconds, the ServerIron ADX concludes that the path is healthy.

- Otherwise, the ServerIron ADX reattempts the health check by sending another ping. By default, the ServerIron ADX reattempts an unanswered path health check up to three times before concluding that the path is unhealthy.

You can change the maximum number of retries to a value from 3 through 31.

To change the maximum number of FWLB path health check attempts, enter a command such as the following at the firewall level of the CLI.

```
ServerIronADX(config-fw-2)# fw-health-check icmp 20
```

Syntax: [no] fw-health-check icmp *<num>*

The *<num>* parameter specifies the maximum number of retries and can be a number from 3 through 31. The default is 3.

Enabling Layer 4 path health checks for FWLB

By default, the ServerIron ADX performs Layer 3 health checks of firewall paths, but does not perform Layer 4 health checks of the paths. You can configure the ServerIron ADXs in an FWLB configuration to use Layer 4 health checks instead of Layer 3 health checks for firewall paths. When you configure a Layer 4 health check, the Layer 3 (ICMP) health check, which is used by default, is disabled.

NOTE
The Layer 4 health check applies only to firewall paths. The ServerIron ADX always uses a Layer 3 (ICMP) health check to test the path to the router.

When you configure a Layer 4 health check for firewall paths, the ServerIron ADX sends Layer 4 health checks and also responds at Layer 4 to health checks from the ServerIron ADX at the other end of the firewall path.

To configure a Layer 4 health check, specify the protocol (TCP or UDP). Optionally, you also can specify the port:

- UDP – The ServerIron ADX sends and listens for path health check packets on the port you specify. If you do not specify a port, the ServerIron ADX uses port 7777 by default. The port number is used as both the source and destination UDP port number in the health check packets.

- TCP – The ServerIron ADX listens for path health check packets on the port you specify, but sends them using a randomly generated port number. If you do not specify a port, the ServerIron ADX uses port 999 as the destination port by default.

NOTE
You must configure the same Layer 4 health check parameters on all the ServerIron ADXs in the FWLB configuration. Otherwise, the paths will fail the health checks.

To configure a Layer 4 health check for firewall paths, enter a command such as the following at the firewall group configuration level.

```
ServerIronADX(config-fw-2)# fw-health-check udp
```

The command in this example enables Layer 4 health checks on UDP port 7777. This ServerIron ADX sends firewall path health checks to UDP port 7777 and listens for health checks on UDP port 7777.

Syntax: [no] fw-health-check udp | tcp [*<tcp/udp-portnum> <num>*]

The *<tcp/udp-portnum>* parameter specifies the TCP or UDP port and can be a number in one of the following ranges:

- For TCP, from 1 through 65535

  ### NOTE
  Do not use port 80 or port 443 for the FWLB TCP health check. Using port 80 or port 443 affects HTTP and HTTPs traffic.

- For UDP, from 2033 through 65535

  ### NOTE
  Do not use a port number less than 2033 for the FWLB UDP health check.

The *<num>* parameter specifies the maximum number of retries and can be a number from 3 through 31. The default is 3.

Disabling Layer 4 path health checks on individual firewalls and application ports

To disable the Layer 4 health check for an individual application on an individual firewall, enter a command such as the following at the firewall configuration level of the CLI.

```
ServerIronADX(config-rs-FW1)# port http no-health-check
```

The command in this example disables Layer 4 health checks for port HTTP on firewall FW1.

Syntax: [no] no-health-check

FWLB selection algorithms

The following section describes selection algorithms for FWLB.

Hashing based on destination TCP or UDP application port

The ServerIron ADX uses a hash value based on the source and destination IP addresses in a packet to select a path, and thus a firewall, for the packet. After calculating this hash value for a given source-and-destination pair, the ServerIron ADX always uses the same path and firewall for packets containing that source-and-destination pair.

NOTE
If hash-port is configured, hashing includes both source-port and destination-port.

You can configure the ServerIron ADX to also hash based on TCP or UDP port numbers. This is useful in environments where the same source-and-destination pairs generate a lot of traffic and you want to load balance the traffic across more than one firewall.

For example, if you configure the ServerIron ADX to hash based on TCP ports 69 (TFTP) and 80 (HTTP), the ServerIron ADX hashes packets addressed to one of these ports by calculating a hash value based on the source and destination IP addresses and the TCP port number (69 or 80). Since the TCP port numbers are included in the hash calculations for these packets, the calculations can result in packets for port 80 receiving a different hash value (and thus possibly a different path and firewall) than packets for port 69, even though the source and destination IP addresses are the same.

NOTE
The current release supports stateful FWLB only for TCP/UDP applications that do not require multiple simultaneous connections for the same client to the same firewall. For example, you cannot use stateful FWLB for FTP, because this application requires separate simultaneous control and data connections to the firewall. The CLI allows you to specify FTP or any other port, but you might not receive the desired results if the application uses multiple simultaneous connections to the same firewall.

Specifying a list of application ports for use when hashing

To specify a list of TCP/UDP ports for hashing, enter the following commands.

```
ServerIronADX(config)# server fw-group 2
ServerIronADX(config-fw-2)# hash-ports 69 80
```

Syntax: **[no] hash-ports** *<num>* [*<num...>*]

The *<num>* parameters specify TCP or UDP port numbers. You can specify up to 16 port numbers on the same command line.

Overriding the global hash values

By default, the ServerIron ADX uses the hash mask you configure for the firewall group for all hash-based load balancing of firewall traffic. You can override the global hash mask for specific traffic based on source or destination address information.

Here is a CLI example.

```
ServerIronADX(config)# access-list 100 permit ip any 192.168.1.16 0.0.0.15
ServerIronADX(config)# access-list 100 permit ip any 192.168.2.0 0.0.0.255
ServerIronADX(config)# access-list 100 permit ip any 192.168.3.192 0.0.0.63
ServerIronADX(config)# access-list 100 permit ip any 192.168.4.0 0.0.0.255
ServerIronADX(config)# access-list 100 permit ip any 192.168.3.160 0.0.0.31
ServerIronADX(config)# access-list 100 permit ip any 192.168.3.0 0.0.0.127
ServerIronADX(config)# access-list 100 permit ip any 64.129.1.0 0.0.0.255
ServerIronADX(config)# server fw-group-2
ServerIronADX(config-fw-2)# hash-mask 255.255.255.255 0.0.0.0
ServerIronADX(config-fw-2)# policy-hash-acl 100 255.255.255.255 255.255.255.255
```

In this example, you configure FWLB to use the hash mask 255.255.255.255 0.0.0.0.

Also, in this example, FWLB will use the hash mask 255.255.255.255 0.0.0.0 for all traffic *except* the traffic that matches ACL 100.

Syntax: **[no] hash-mask** *<dst-mask>* *<src-mask>* | *<dst-ipv6-mask>* *<src-ipv6-mask>*

NOTE
IPv4 and IPv6 address formats cannot be mixed. Addresses must be entered in the same format.

The *<dst-mask>* parameter specifies the IPv4 destination address mask.

The *<src-mask>* parameter specifies the IPv4 source address mask.

The *<dst-ipv6-mask>* parameter specifies the IPv6 destination address mask.

The *<src-ipv6-mask>* parameter specifies the IPv6 source address mask.

Syntax: **[no] server policy-hash-acl** *<acl-id>* *<dst-mask>* *<src-mask>* | *<dst-ipv6-mask>* *<src-ipv6-mask>*

The *<acl-id>* parameter specifies a standard or extended ACL identifier.

The *<dst-mask>* parameter specifies the IPv4 destination address mask.

The *<src-mask>* parameter specifies the IPv4 source address mask.

The *<dst-ipv6-mask>* parameter specifies the IPv6 destination address mask.

The *<src-ipv6-mask>* parameter specifies the IPv6 source address mask.

Configure each entry in the ACL to permit the addresses for which you want to override the global hash mask.

Configuring weighted load balancing

You can assign weights to your firewalls to bias the load balancing in favor of certain firewalls.

Weight

The weight you assign to a firewall determines the percentage of the current connections that are given to that firewall. For example, in a configuration with five firewalls of various weights, the percentage of connections is calculated as follows:

- Weight fwall1 = 7
- Weight fwall2 = 8
- Weight fwall3 = 2
- Weight fwall4 = 2
- Weight fwall5 = 5

The total weight of all the firewalls is 24

The result is that fwall1 gets 7/24 of the current number of connections, fwall2 gets 8/24, server3 gets 2/24, and so on. If a new firewall, fwall6, is added with a weight of 10, the new firewall gets 10/34.

If you set the weight so that your fastest firewall gets 50 percent of the connections, it will get 50 percent of the connections at a given time. Because the firewall is faster than others, it can complete more than 50 percent of the total connections overall because it services the connections at a higher rate. Thus, the weight is not a fixed ratio but adjusts to firewall capacity over time.

The default weight for firewalls is 1.

Assigning weights to firewalls

To assign weights to firewalls, enter the following commands.

```
ServerIronADX(config)# server fw-name fw1
ServerIronADX(config-rs-fw1)# weight 7
ServerIronADX(config-rs-fw1)# server fw-name fw2
ServerIronADX(config-rs-fw2)# weight 8
ServerIronADX(config-rs-fw2)# server fw-name fw3
ServerIronADX(config-rs-fw3)# weight 2
ServerIronADX(config-rs-fw3)# server fw-name fw4
ServerIronADX(config-rs-fw4)# weight 2
ServerIronADX(config-rs-fw4)# server fw-name fw5
ServerIronADX(config-rs-fw5)# weight 5
```

These commands assign weights to five firewalls. The ServerIron will load balance new connections to the firewalls based on their relative weights.

Syntax: **[no] weight** *<least-connections-weight>*

The *<least-connections-weight>* parameter assigns a weight to the firewall. This weight determines the percentage of new connections the firewall receives relative to the other firewalls.

NOTE
The **weight** command has a second parameter, *<response-time-weight>*. This parameter is valid for real servers in SLB configurations but is not valid for FWLB.


Denying FWLB for specific applications

You can deny FWLB for specific applications while still permitting FWLB for other applications. For example, you can deny FWLB for HTTP traffic (TCP port 80) while still providing FWLB for other types of traffic.

This feature is useful when your network is configured to send all traffic for a given application to the same firewall. For example, Figure 25 shows a network in which the routers are configured to send all HTTP traffic through firewall FW1.

FIGURE 25   **FWLB denied for application traffic**
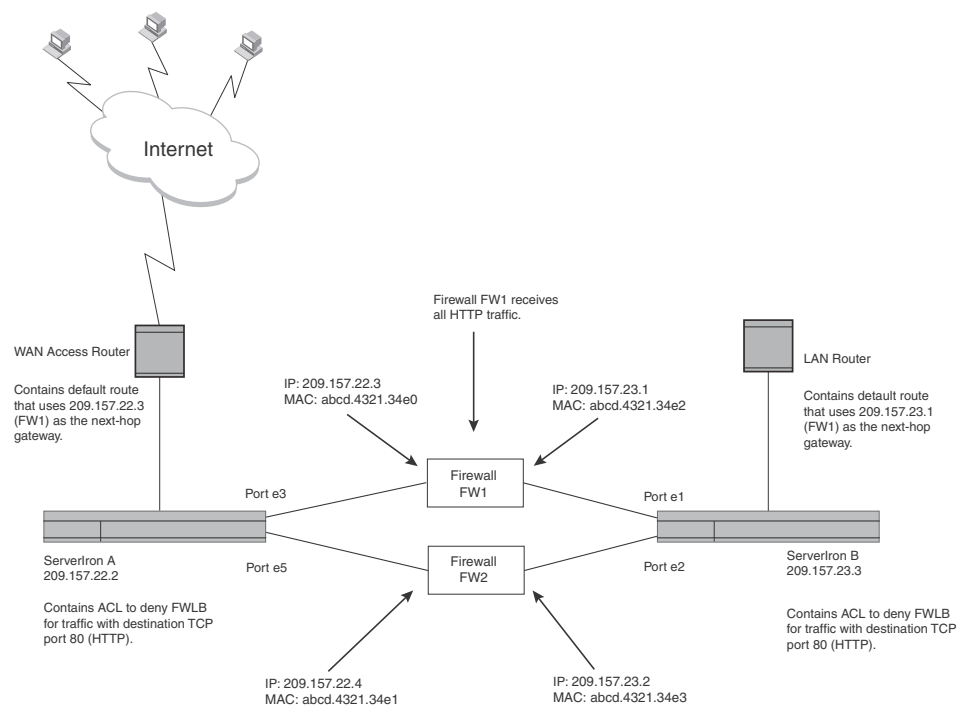
In this example, the network is configured as follows:

- The WAN access router has a default route that identifies IP address 209.157.22.3 on FW1 as the next-hop gateway.

- The LAN router has a default route that identifies IP address 209.157.23.1 (also on FW1) as the next-hop gateway.

- ServerIron ADX A has an extended ACL at the firewall group configuration level that denies FWLB for packets addressed to destination TCP port 80.

- ServerIron ADX B has an extended ACL at the firewall group configuration level that denies FWLB for packets from source TCP port 80.

Notice that the routers use default routes to send traffic to a specific firewall. However, the default routes do not necessarily determine the firewall to which the ServerIron ADX sends the traffic. When the ServerIron ADX performs load balancing for a packet and selects a firewall for the traffic, the ServerIron ADX also changes the destination MAC address of the packet to the MAC address of the firewall selected by the ServerIron ADX. For example, in Figure 25, if ServerIron ADX A selects firewall FW2 for a packet, the ServerIron ADX changes the destination MAC address of the packet to abcd.4321.34e1, the MAC address of firewall FW2's interface with ServerIron ADX A. As a result, even if the WAN access router addresses a packet to the MAC address for firewall FW1, the ServerIron ADX does not send the packet to firewall FW1 unless the load balancing mechanism selects that firewall. In either case, the ServerIron ADX changes the destination MAC address of the packet.

If you want to ensure that all packets for an application go to a specific firewall (as specified in the default route on the router), you must deny FWLB service for that application. For example, if you have configured firewall FW1 to collect statistics on HTTP traffic and you therefore want to send all the HTTP traffic to firewall FW1, you must disable FWLB for HTTP traffic. To disable FWLB for an application, configure an extended ACL at the firewall group configuration level.

NOTE
When you configure an ACL at the firewall group configuration level, a deny action does not cause the ServerIron ADX to drop the denied packet. In this type of configuration, a deny action denies FWLB service for the packet, so that the ServerIron ADX leaves the destination MAC address of the packet unchanged.

NOTE
This section focuses on using extended ACLs to deny FWLB based on TCP or UDP port. However, you also can use standard ACLs at the firewall group configuration level to deny FWLB based on IP address.

Configuration guidelines

Consider the following:

- Configure extended ACLs at the firewall group configuration level to deny FWLB for specific applications.

- Configure a permit ACL to allow all applications. Once you configure an ACL, the default action changes from permit to deny. As a result, if you do not configure the permit ACL for all traffic types, FWLB is denied for all traffic. Make sure the permit ACL for all traffic is the last ACL, after all the deny ACLs.

- Configure the deny ACLs for each direction of traffic for which you want to deny FWLB. In Figure 25, configure a deny ACL on ServerIron ADX A to deny FWLB for packets addressed to destination TCP port 80 (HTTP). To deny FWLB for the return traffic, configure a deny ACL on ServerIron ADX B to deny packets from source TCP port 80.

Denying FWLB

To deny FWLB for an application, enter commands such as the following. These commands configure the ServerIron ADXs in Figure 25 to deny FWLB for HTTP traffic, in both directions. On ServerIron ADX A, FWLB is denied for traffic addressed to TCP port 80. On ServerIron ADX B, FWLB is denied for traffic from TCP port 80.

ServerIron ADX A commands

The following commands configure three ACL entries. The first entry denies FWLB for packets addressed to TCP port 80 (HTTP). The second ACL permits FWLB for all TCP applications. Packets that do not match the first ACL entry match the second ACL entry and are provided with FWLB. The third ACL permits FWLB for all UDP applications. The last two commands change the CLI level to the firewall group configuration level and apply ACL 101 to the firewall group.

```
ServerIronADXA(config)# access-list 101 deny tcp any any eq http
ServerIronADXA(config)# access-list 101 permit tcp any any
ServerIronADXA(config)# access-list 101 permit udp any any
ServerIronADXA(config)# server fw-group 2
ServerIronADXA(config-fw-2)# acl-id 101
```

Syntax: [no] access-list *<num>* deny | permit *<ip-protocol> <source-ip>* | *<hostname>*
<wildcard> [*<operator> <source-tcp/udp-port>*] *<destination-ip>* | *<hostname>*
<wildcard> [*<operator> <destination-tcp/udp-port>*]
[precedence *<name>* | *<num>*] [tos *<name>* | *<num>*] [log]

Syntax: [no] acl-id *<acl -id>*

The *<acl-id>* parameter specifies a standard or extended ACL identifier.

ServerIron ADX B commands

These following commands are the same as the commands on ServerIron ADX A, except the first ACL entry matches on TCP port 80 (eq http) as the destination TCP port on ServerIron ADX A, but matches as the source TCP port on ServerIron ADX B.

```
ServerIronADXB(config)# access-list 101 deny tcp any eq http any
ServerIronADXB(config)# access-list 101 permit tcp any any
ServerIronADXB(config)# access-list 101 permit udp any any
ServerIronADXB(config)# server fw-group 2
ServerIronADXB(config-fw-2)# acl-id 101
```

Configuring failover tolerance in IronClad configurations

By default, failover from the active ServerIron ADX to the standby ServerIron ADX in an IronClad configuration occurs if a path link on the active ServerIron ADX becomes unavailable. If all the path links are stable, failover is an uncommon event. However, an unreliable link can cause frequent failover. For example, if a link on a firewall flaps (goes up and down) frequently, the flapping can cause frequent, unnecessary failovers.

You can reduce the frequency of such failovers by specifying a path link tolerance for firewall paths and for router paths. The tolerance specifies the minimum number of such paths that must be good in order for the active ServerIron ADX to remain active. Only if the number of paths is less than the configured minimum and less than the number of available paths on the other ServerIron ADX does failover occur. If the number of paths remains equal on each ServerIron ADX, even if some paths are unavailable on each ServerIron ADX, failover does not occur.

The default failover tolerance for firewall paths is one half the configured firewall paths. The default tolerance for router ports is one half the configured router ports.

To change the minimum number of paths required on a ServerIron ADX, use the following method.

NOTE
The minimum number of required paths must match on each ServerIron ADX in an active-standby pair. For example, if you specify one router path and three firewall paths as the minimum on the active ServerIron ADX, you must configure the same minimums on the standby ServerIron ADX.

To specify the minimum number of paths required on a ServerIron ADX, enter the following commands.

```
ServerIronADX(config)# server fw-group 2
ServerIronADX(config-fw-2)# prefer-router-cnt 1
ServerIronADX(config-fw-2)# prefer-cnt 3
```

This example specifies that a minimum of one router path and three firewall paths must be available for the ServerIron ADX to remain active. Thus, if the ServerIron ADX has four firewall paths, one path can be unavailable and the ServerIron ADX will remain the active ServerIron ADX.

Syntax: [no] prefer-router-cnt *<num>*

Syntax: [no] prefer-cnt *<num>*

For each command, the *<num>* parameter specifies the minimum number of paths required.